PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

LOTERÍA DE BOYACÁ
2024

Contenido

INTRODUCCIÓN

Mediante la adopción del Modelo de Seguridad y Privacidad en la Lotería de Boyacá se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

La implementación del plan de Seguridad y Privacidad de la Información en la Entidad está determinada por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de esta, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

GLOSARIO

- **Acceso a la Información Pública:**
  Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

- **Activo:**
  En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma. (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Activo de Información:**
  En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

- **Archivo:**
  Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

- **Amenazas:**
  Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Análisis de Riesgo:**
  Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Auditoría:**
  Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- **Autorización:**

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

- **Bases de Datos Personales:**
  Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

- **Ciberseguridad:**
  Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

- **Ciberespacio:**
  Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- **Control:**
  Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Datos Abiertos:**
  Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

- **Datos Personales:**
  Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos Personales Públicos:**
  Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos,

gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

- **Datos Personales Privados:**
  Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

- **Datos Personales Mixtos:**
  Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

- **Datos Personales Sensibles:**
  Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

- **Declaración de aplicabilidad:**
  Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

- **Derecho a la Intimidad:**
  Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- **Encargado del Tratamiento de Datos:**
  Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

- **Gestión de incidentes de seguridad de la información:**
  Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Información Pública Clasificada:**
  Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- **Información Pública Reservada:**
  Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- **Ley de Habeas Data:**
  Se refiere a la Ley Estatutaria 1266 de 2008.

- **Ley de Transparencia y Acceso a la Información Pública:**
  Se refiere a la Ley Estatutaria 1712 de 2014.

- **Mecanismos de protección de datos personales:**
  Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

- **Plan de continuidad del negocio:**
  Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- **Plan de tratamiento de riesgos:**
  Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Privacidad:**
  En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades

destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- **Registro Nacional de Bases de Datos:**
  Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

- **Responsabilidad Demostrada:**
  Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

- **Responsable del Tratamiento de Datos:**
  Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

- **Riesgo:**
  Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información:**
  Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Sistema de Gestión de Seguridad de la Información SGSI:**
  Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

- **Titulares de la información:**
  Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

- **Tratamiento de Datos Personales:**

Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

- **Trazabilidad:**
  Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

- **Vulnerabilidad:**
  Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

- **Partes interesadas (Stakeholder):**
  En el mundo de los negocios, los stakeholders son aquellos individuos o grupos que tienen interés e impacto en una organización y en los resultados de sus acciones. Algunos de los ejemplos más comunes de stakeholders son los empleados, los accionistas, los clientes, los proveedores, los gobiernos y las comunidades.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Generar el Plan de Seguridad y Privacidad de la Información de la Lotería de Boyacá para la vigencia 2024 – 2026.

1.2. OBJETIVOS ESPECÍFICOS

- Promover el uso de mejores prácticas de seguridad de la información, para garantizar la seguridad de la información que maneja la Lotería de Boyacá.
- Determinar los niveles de privacidad y seguridad de la información al interior de la Lotería de Boyacá, para optimizar su organización y disponibilidad.
- Orientar a la administración de la Entidad en la construcción de políticas de manejo de datos, para optimizar la seguridad de la información que se procesa en su interior.
- Implementar mejores prácticas de seguridad, para identificar vulnerabilidades al interior de la infraestructura tecnológica de la Lotería de Boyacá.

2. MARCO NORMATIVO

INVENTARIO DE MARCOS DE REFERENCIA Y NORMATIVA APLICABLES				
ID	**Nombre**	**Número/Año**	**Descripción**	**Artículo o artículos que aplican**
Normativa Estatal				
1	Ley de Transparencia	Ley 1712 de 2014	Herramienta normativa que regula el ejercicio del derecho fundamental de acceso a la información pública en Colombia.	Todo
2	Ley de Protección de Datos Personales.	Ley 1581 de 2012	Ley que complementa la regulación vigente para la protección del derecho fundamental que tienen todas las personas naturales a autorizar la información personal que es almacenada en las bases de datos o archivos, así como su posterior actualización y rectificación.	Todos
3	Ley de Habeas Data	Ley Estatutaria 1266 de 2008	Por la cual se dictan disposiciones generales del **habeas data** y se regula el manejo de la información contenida en bases de datos personales.	Todos
4	Modelo de Seguridad y Privacidad de la Información	Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.	Todos
Normativa de Calidad				
5	Norma ISO/IEC 27000	Estándar del Sistema de Gestión de Seguridad de la Información		Todos

3. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Lotería de Boyacá actualmente se encuentra con el reto de adaptarse a un entorno cada vez más cambiante e impredecible, con un alto nivel de competencia y de exigencia para mejorar, crecer y desarrollarse de acuerdo con las necesidades del mercado de los juegos de azar.

En esa necesidad de tener clientes satisfechos y ser cada vez más competitivos debe apoyarse en herramientas como el modelo PHVA (Planear, hacer, actuar y verificar), el cual permite mejorar continuamente los procesos de una organización, además, se caracteriza por su efectividad y eficiencia, al ser un modelo dinámico y flexible, el cual puede ser aplicado en diferentes servicios o productos que tiene la Entidad, de igual forma, en los procesos del sistema de gestión. Su gran importancia radica en ayudar a reducir costos, mejorar la productividad y en la supervivencia de la organización en un mercado cada vez más cambiante.

3.1. PLANEAR

En esta primera fase se realiza un estudio de la situación actual de la Lotería de Boyacá, desde el punto de vista de la seguridad de la información, es necesario estimar las medidas que se van a implementar en función de las necesidades detectadas, determinando así el alcance del MSPI y la política de seguridad.

Se debe tener en cuenta que no toda la información de la Lotería de Boyacá tiene el mismo valor en cuanto a los tres pilares (confidencialidad, integridad y disponibilidad), e igualmente, no toda la información está sometida a los mismos riesgos. Por ello, una de las actividades importantes dentro de esta fase es la realización de un Análisis de Riesgos que ofrezca una valoración de los activos de información y las vulnerabilidades a las que están expuestos. Así mismo, se hace necesario el análisis de dichos riesgos con el fin de evaluar los posibles impactos para la Entidad y con base en ello, establecer planes de acción con miras a minimizar dichos riesgos.

Toda esta identificación, parte de un levantamiento de información referente a los activos de información, tal como lo define la ley 1712 de 2014 dentro de su artículo 13, el cual va a permitir clasificar los activos a los que se les debe brindar mayor protección, pues identifica claramente sus características y rol al interior de un

proceso, así como la información que la entidad tiene y debe manejar para cumplir con la misión institucional.

Las actividades por realizar para obtener un inventario de activos serán:

Definición: Consiste en determinar qué activos de información van a hacer parte del inventario de la Entidad y para esta tarea debe existir un equipo que realice la gestión de activos de información al interior de la misma, por medio del líder de cada proceso.

Revisión: Se refiere a la verificación que se lleva a cabo para determinar si un activo de información continua o no siendo parte del inventario, o si los valores de evaluación asignados en el inventario y clasificación de activos de Información deben ser modificados.

Actualización: Una vez se ha definido qué cambios se realizarían en el inventario, desde cada proceso, se procede a actualizar el inventario de activos de información por medio del procedimiento definido por planeación para tal efecto.

Publicación: El inventario de activos de información debe ser un documento clasificado como “Confidencial”, como lo define **MinTIC**, pero para poder dar cumplimiento a la ley de transparencia, en el cual se define que se debe publicar en formato editable, la Entidad adelantará una revisión de cada registro y procederá a eliminar los registros que sean clasificados o reservados o que posean información específica de la Lotería de Boyacá, la cual no pueda ser publicada de esa manera, como por ejemplo, nombres de servidores, direcciones IP, nombres de Sistemas de Información, entre otros, y los definidos por la ley. En ese sentido, se generan dos documentos, los cuales van a tener audiencias diferentes dependiendo de la clasificación que se requiera.

3.1.1. CONTEXTO DE LA ENTIDAD

En general, esta fase consiste en entender el contexto de la Lotería de Boyacá como entidad pública, apoyándose en su visión, en su estructura jerárquica, en sus sistemas de información y en sus grupos de interés, e identificar los requisitos y expectativas de la seguridad de la información desde la perspectiva del cumplimiento de los requerimientos de usuario o parte interesada. Para ello es importante comprender los procesos y procedimientos en los que se soporta para cumplir sus objetivos, mirar el contexto interno y externo de la Entidad, definir los flujos de información con cada una de las partes interesadas y en general, comprender a la entidad como un Sistema, dando como resultado el entendimiento de la Entidad y a partir de eso, la definición del alcance del Sistema de Seguridad de Información, los objetivos del MSPI y la Política de seguridad de la información en la Lotería de Boyacá.

3.1.2. ALCANCE DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

EL MSPI es aplicable a los activos de información de todos los procesos de la Lotería de Boyacá, verificándolo y aplicándolo en cada dependencia u oficina, y comprende las políticas, procesos, procedimientos y controles para la preservación de confidencialidad, integridad y disponibilidad de la información.

3.1.3. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad y privacidad de la información es la afirmación general que representa la posición de administración de la Lotería de Boyacá, con el fin de proteger los activos de la información (los servidores públicos, contratistas, pasantes, los procesos, las tecnologías de la información incluido el hardware y el software), que soportan los procesos de la entidad y apoyan la implementación del sistema de gestión de seguridad de la información, por medio de la generación y publicación de políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información, que conlleve a establecer un mecanismo que facilite el cumplimiento, disponibilidad y confidencialidad de la información intercalada en todas las áreas de la empresa.

La Lotería de Boyacá tiene como objetivos de seguridad de la información los siguientes ítems:

- Minimizar el riesgo en todos los procesos, especialmente en los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los servidores públicos, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los servidores públicos, terceros, practicantes y clientes de la Lotería de Boyacá.
- Garantizar la continuidad de los procesos de la Lotería de Boyacá frente a incidentes.

COMPROMISO ESPECIFICO DE LA SEGURIDAD DIGITAL

La Lotería de Boyacá establecerá la seguridad digital como una responsabilidad institucional y un compromiso de todo el personal, contemplando los activos de información de la entidad, su clasificación según su naturaleza - información, software, hardware y/o componentes de red, estableciendo la Infraestructura Tecnológica Crítica de la Entidad, identificando los riesgos de seguridad digital, mediante la metodología dispuesta por el DAFP y el Ministerio de TIC.

Para esto se implementará el Modelo de Seguridad y Privacidad de la Información MSPI con las herramientas que el Ministerio de TIC destine para ello, el cual integra en cada una de sus fases, tareas asociadas a la identificación, gestión, tratamiento y mitigación de riesgos de seguridad digital con respecto a misión de la entidad, con lo que se evaluará el desempeño del MSPI, a través de la aplicación de esta política de seguridad y privacidad de la información, la ejecución de los controles definidos en la declaración de aplicabilidad y el monitoreo de los indicadores de seguridad de la información.

3.1.4. INVENTARIO DE ACTIVOS DE INFORMACIÓN

Un activo de información, según la ley 1712 de 2014, es el elemento de información que la entidad recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentra presente en forma impresa, escrita, en papel, trasmitida por cualquier medio electrónico o almacenado en equipos de

cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes.

3.1.5. ANÁLISIS DE BRECHA

El análisis de brecha busca generar un diagnóstico relativo a la seguridad de la información basado en la identificación de diferencias entre el estado actual y el estado ideal de la seguridad de la información en la Lotería de acuerdo con los requerimientos exigidos en la norma ISO 27001:2013 y el modelo de seguridad y privacidad de la Información – MSPI.

Las fases para realizar una metodología de diagnóstico de seguridad de la información son:

- Revisión del cumplimiento de las exigencias de la Norma ISO 27001 en concordancia con el modelo de seguridad y privacidad de la Información - MSPI, respecto a la Seguridad de la Información, la gestión de los riesgos, el análisis de vulnerabilidades y el seguimiento a las mismas.

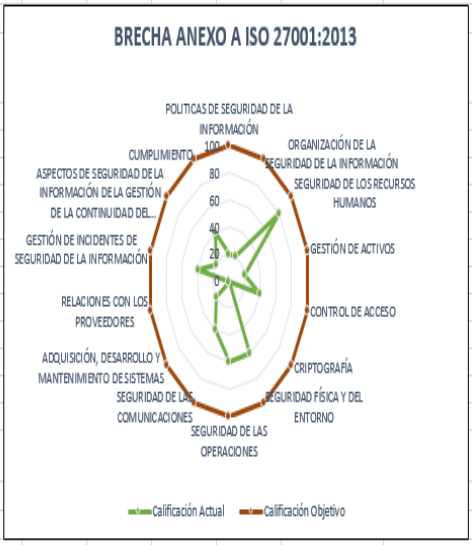
- Revisión de los controles existentes que apliquen a la seguridad de la información en la Lotería de Boyacá.

- Identificar requisitos faltantes (Políticas, procedimientos, controles), los cuales son exigidos por la norma ISO 27001 y por los modelos del MinTic – MSPI.

En cumplimiento con lo establecido por el ministerio TIC, se va a usar la herramienta de diagnóstico de seguridad y privacidad de la información elaborada por ellos, la cual arroja un resultado que permite a cada entidad visualizar los diferentes dominios de la norma, evaluar las falencias y a partir de eso, generar un plan de seguridad de la información para ser desarrollado al interior de la misma y dar cumplimiento con lo estipulado en el manual de gobierno digital en sus diferentes componentes. Al aplicar la herramienta, con corte a Diciembre de 2023, se generaron los siguientes resultados:

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	80	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	20	100	INICIAL
A.9	CONTROL DE ACCESO	40	100	REPETIBLE
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	60	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	60	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	40	100	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	20	100	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	0	100	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	40	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	100	INICIAL
A.18	CUMPLIMIENTO	40	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		33	100	REPETIBLE



Fuente: Autodiagnóstico MSPI con corte a diciembre de 2023

3.1.6. DOCUMENTACIÓN DE PROCEDIMIENTOS

Durante esta fase se identificarán y documentarán procedimientos necesarios para dar cumplimiento a la norma ISO 27001 y a las necesidades propias que la Lotería de Boyacá requiere, garantizando un adecuado funcionamiento del Sistema de Gestión de Seguridad de la Información - MSPI. Actualmente la Dirección TIC cuenta con los siguientes procedimientos:

Id	Procedimiento	Objetivo
Pro-01	Gestión de sistemas	Planeación y Ejecución del Plan Estratégico de Tecnologías de la Información y las Comunicaciones.
Pro-02	Realización de copias de seguridad	Ofrecer la capacidad de recuperación de la información ante posibles pérdidas
Pro-03	Instalación y Control de Licenciamiento de Software	Establecer los pasos a seguir para distribuir adecuadamente y de manera controlada las licencias de software disponibles para los equipos de cómputo de la Lotería de Boyacá
Pro-04	Mantenimiento Preventivo y	Evitar o mitigar las consecuencias de los fallos en equipos de cómputo, buscando

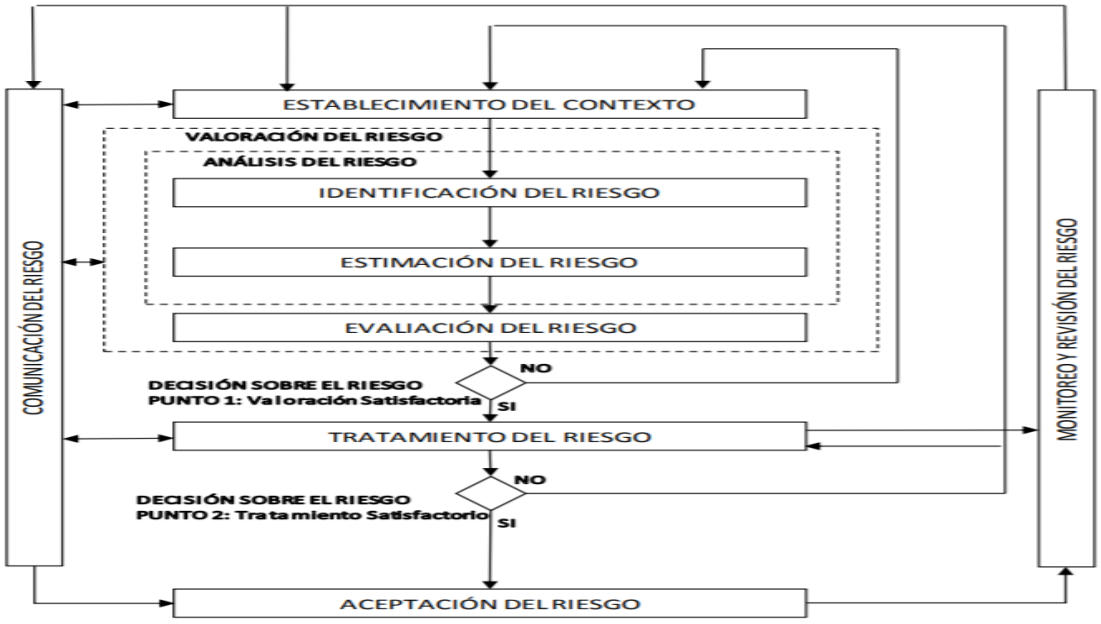
	Correctivo de Hardware	prevenir las incidencias antes de que estas ocurran
Pro-05	Soporte Técnico a usuarios de Software	Prevenir y dar solución a problemas que presenten los usuarios durante el uso del software que posee la Lotería de Boyacá
Pro-06	Soporte Técnico al Sorteo	Prevenir y dar solución a problemas que se presenten con los equipos de cómputo, software y comunicaciones que se usan e intervienen para la realización del sorteo de la lotería.

En este sentido, la entidad entra a valorar cada uno de los procedimientos con el fin de hacer la revisión desde la perspectiva del SGSI-MSPI, acoplarlos a las nuevas necesidades y crear los nuevos procedimientos que permitan dar cumplimiento a los controles definidos por la norma y por el quehacer de la entidad.

3.1.7. ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión de riesgos de seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento, el cual es adoptado desde la Dirección TIC de la Lotería de Boyacá. El proceso de Gestión del Riesgo en la Seguridad de la Información puede ser iterativo para las actividades de valoración del riesgo y/o el tratamiento del mismo. Esto permite que al realizar la valoración del riesgo se pueda incrementar la profundidad y el detalle de la valoración en cada iteración.

Proceso para la administración del riesgo en seguridad de la información:



Fuente: NTC-ISO/IEC 27005

El contexto se establece como primera medida, luego se realiza la valoración del riesgo y si esta suministra información suficiente para determinar de manera eficaz las acciones que se necesitan para modificar los riesgos a un nivel aceptable entonces la labor está terminada y se sigue con el tratamiento del riesgo. Si la información no es suficiente, se llevará a cabo otra iteración de la valoración del riesgo con un contexto revisado.

3.1.8. SENSIBILIZACIÓN Y FORMACIÓN DE FUNCIONARIOS

Es importante que la Lotería de Boyacá establezca lineamientos para la construcción un plan de capacitación, sensibilización y comunicación de la seguridad de la información que cubra la totalidad de los funcionarios de la Entidad, asegurando que cada uno cumpla con sus roles y responsabilidades de seguridad y privacidad de la información. Para adelantar este plan es necesario:

- Evidenciar las problemáticas existentes en temas de seguridad de la información en la Lotería de Boyacá.
- Definir los temas para la capacitación en seguridad de la información, teniendo en cuenta la población objetivo.
- Construir o preparar materiales para apoyar la sensibilización y capacitación en seguridad de la información.
- Monitorear el plan de sensibilización y capacitación.

3.1.9. GESTIÓN DE RECURSOS PARA EL SGSI-MSPI

Es compromiso de la Dirección de la Lotería de Boyacá, garantizar los recursos tanto presupuestales como de personal para la implementación exitosa del SGSI - MSPI.

3.1.10. SOPORTE

3.1.10.1. RECURSOS

La Dirección de la Lotería de Boyacá con el apoyo de la Oficina de Sistemas deben planificar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de la Seguridad de la Información.

3.1.10.2. COMPETENCIA

Es la capacidad con la que se aplican los conocimientos y las habilidades en la Entidad con el fin de conseguir los resultados previstos en cuanto a la implementación del Sistema de Gestión de la Seguridad de la Información. Las competencias se determinan a partir de la identificación de necesidades en la Entidad. Es importante involucrar en la identificación de necesidades a todo el personal que labora en la Entidad, así como a terceros que interactúan con su línea de negocio. A continuación, se describen las siguientes competencias:

Perfil ocupacional	Competencias
Ejecutivos	• Deben conocer y entender las leyes y directivas que forman la base del programa de seguridad, también deben comprender el liderazgo que su rol tiene y que son el ejemplo a seguir de todas las demás unidades.
Profesionales en seguridad de la Información y sistemas de información	• Son los asesores expertos en seguridad, deben estar bien preparados en políticas de seguridad y buenas prácticas. • Deben ser profesionales con aptitud para aplicar y promover metodologías actualizadas que conduzcan a la práctica de una cultura de la información; capaces de discernir entre las

Perfil ocupacional	Competencias
	ventajas y desventajas asociadas con el diseño y administración de políticas de seguridad para los recursos informáticos de la Entidad. • Deben diseñar estrategias que puedan garantizar la seguridad de los recursos informáticos de tal forma que se conviertan en un valor agregado en los procesos de la Entidad, basado en estándares nacionales e internacionales y aspectos éticos y legales que rigen la seguridad de la información. • Evaluar y coordinar la implementación de controles específicos de seguridad de la información para los nuevos sistemas de información o servicios tecnológicos. • Deben entender bien las políticas de seguridad, así como también conocer sobre los controles de seguridad y la relación que tienen con los sistemas que maneja la Lotería de Boyacá.
Administradores de sistemas y personal de soporte	• Estos funcionarios deben tener un buen nivel de preparación a nivel técnico de seguridad (implementación y prácticas de seguridad efectivas) para soportar las operaciones críticas del Entidad de manera apropiada. • Garantizar la definición, monitoreo, accesibilidad, funcionalidad y mantenimiento de las redes y servidores del Entidad. • Colaborar en la correcta ejecución y control de los procesos de creación de respaldos de información y/o recuperación. • Registrar y controlar el inventario de infraestructura de la de la Lotería de Boyacá. • Supervisar el correcto funcionamiento de la plataforma tecnológica de la Entidad a través de sistemas de monitoreo, a fin de prevenir interrupciones en el servicio y gestionar las acciones que permitan garantizar su adecuado funcionamiento.
Usuarios finales	• Requieren de un alto grado de sensibilización sobre la seguridad y las reglas de comportamiento adecuadas con los sistemas que tienen a disposición. • Respetar y seguir las normas y procedimientos definidos en la política de seguridad de la información.

Perfil ocupacional	Competencias
	• Notificar al responsable de seguridad de la información las anomalías o incidentes de seguridad, así como las situaciones sospechosas. • Mantener la confidencialidad, integridad y disponibilidad de la información. • Hacer un buen uso de los activos de información de la Entidad.

3.2. HACER

3.2.1. OPERACIÓN

En esta fase se lleva a cabo el establecimiento de los controles de seguridad escogidos en la fase anterior junto con los seguimientos, actualizaciones y procesos de mejora propios de este ítem. Es importante ejecutar el Plan de Sensibilización y Capacitación (incluido en el plan de capacitación de la entidad) propuesto en fase de Planeación el cual conlleva a la concientización y/o formación del personal de la Lotería de Boyacá en el conocimiento y aplicación de los controles implantados en pos de garantizar la seguridad de la información en la entidad y dejar claro el rol que cada funcionario, contratista o grupo de interés desempeña y sobre todo, el buscar la colaboración de cada una de las personas como parte activa del sistema.

3.2.2. MÉTRICAS DE EFICACIA DE LOS CONTROLES Y DEL SGSI-MSPI

Toda vez que el SGSI-MSPI es un sistema de mejora continua, hay necesidad de definir parámetros precisos para evaluar los controles ejecutados y en sí, la evolución del sistema en términos de justificar cada una de las acciones tomadas o en su defecto redirigir dichas acciones hacia la consecución de procesos más eficientes y efectivos. Por tal razón, se debe definir un sistema de métricas e indicadores que permitan obtener resultados de la ejecución del sistema, los cuales conllevan a medir la eficacia o eficiencia de los controles implementados, la consecución de objetivos y en general el nivel de implementación del sistema frente a la madurez de este.

3.2.3. GESTIÓN DE FUNCIONAMIENTO NORMAL DEL SGSI-MSPI

La Lotería de Boyacá debe adoptar el Sistema de Gestión de Seguridad de la Información SGSI-MSPI, como parte integral y trasversal de la Entidad y como tal, debe gestionar las operaciones del Sistema mediante el seguimiento y revisión continuo de todo el sistema, la evaluación y toma de decisiones frente a los resultados definidos por las métricas e indicadores adoptados y generar planes de mejoramiento para optimizar los resultados y suplir las falencias encontradas, todo esto confluyendo en auditorías internas y externas que demuestren la fortaleza o no del sistema desarrollado.

3.2.4. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Lotería de Boyacá implementará un plan de gestión de incidentes**,** creado para detectar y gestionar un incidente, definido como toda aquella actividad ejecutada como resultado de eventos adversos e inesperados que ocurran como resultado de controles fallidos o inexistentes, teniendo en cuenta las directrices adelantadas por MINTIC, la Policía Nacional y los entes competentes en esta área.

3.3. VERIFICAR

3.3.1. EVALUACIÓN DEL DESEMPEÑO

La Lotería de Boyacá debe proveer mecanismos que le permitan evaluar la eficacia y éxito de los controles implementados. Por este motivo tendrán especial importancia los registros (evidencias) que dejan los diferentes controles, así como los indicadores que permiten verificar el correcto funcionamiento del SGSI-MSPI. Los mecanismos a tener en cuenta son:

- Implementar procedimientos y demás controles de supervisión y control para determinar cualquier violación, procesamiento incorrecto de datos y determinar si las actividades de seguridad se desarrollan de acuerdo con lo previsto.

- Revisar la eficacia del SGSI-MSPI mediante la evaluación y análisis de las métricas definidas para tal fin, dentro del tiempo establecido por la Lotería de Boyacá.

- Revisar el estado de los activos de información, manteniendo actualizada la matriz correspondiente y la matriz de riesgos.

- Revisar la evaluación de riesgos, actualizando este Plan de tratamiento de riesgos y plan de seguridad, de ser necesario y/o dentro del tiempo establecido por la empresa. (Anualmente)

- Realizar Auditorías internas planificadas.

- Adelantar revisiones por parte de la alta dirección para asegurar el funcionamiento del SGSI-MSPI e identificar oportunidades de mejora.

- Mantener los registros de las actividades e incidentes que puedan afectar la eficacia del SGSI-MSPI.

3.4. ACTUAR

3.4.1. MEJORA CONTINUA

En esta fase se llevarán a cabo las labores de mantenimiento y mejora del sistema de gestión de seguridad de información, seguimiento a riesgos, análisis de vulnerabilidades, hacking ético, así como las labores de mejora y de corrección si, tras la verificación, se ha detectado algún punto débil. Esta fase se puede llevar en paralelo con la verificación y se despliega al detectarse la deficiencia o hallazgo negativo, no esperando a adelantar una fase de verificación programada para comenzar con las tareas de mejora continua y corrección. Para lograrlo, la Lotería de Boyacá debe:

- Implementar y documentar en el SGSI-MSPI las mejoras identificadas.
- Tomar medidas correctivas y preventivas y aplicar las mejores prácticas sobre incidentes de seguridad, provenientes de experiencias de seguridad propias y de terceros documentadas.
- Comunicar las actividades y mejoras a todos los grupos de interés.
- Garantizar que las mejoras cumplan los objetivos previstos y que estén enfocadas a las necesidades y requerimientos de la Entidad.

4. VIOLACIONES A LAS POLITICAS DE SEGURIDAD

La Lotería de Boyacá con el fin de evitar violaciones a las políticas de seguridad promueve el uso responsable de las comunicaciones, debido a que los activos de información y los equipos informáticos son recursos importantes para la empresa, dicho lo anterior, se deben tomar acciones apropiadas para asegurar la información estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como el fraude, sabotaje, hackers, interrupción de servicio etc.

Con el propósito de mejorar, se consideran las siguientes actividades como violaciones a las políticas de seguridad:

- Enviar corro electrónico no solicitado o Spam
- Envió de correo con contenidos inapropiados(pornografía)
- Utilización indebida de la internet, es decir, navegación en páginas con contenidos inapropiados, juegos en línea o cualquier otro sitio con fines diferentes a los laborales.
- Instalación o ejecución de software no autorizados.
- Traslado o instalación de nuevos equipos a la red sin la autorización ni el procedimiento establecido por el área de Sistemas.
- Dañar los equipos o la infraestructura informática.
- Utilizar cualquiera de los recursos informáticos de la Lotería de Boyacá para fines diferentes a las funciones contractuales.
- Utilizar cualquier tipo de software para fines maliciosos o intrusos como escáner de puertos, keyloggers, sniffers, entre otros.
- Utilizar cualquier técnica de hacking hacia cualquiera de los recursos tecnológicos de la Lotería de Boyacá entre los que se incluye: ataque dos, spoofing, broadcast storm.
- Conseguir acceso no autorizado a cualquier equipo o información.
- Conseguir acceso no autorizado a los recursos compartidos, almacenados en los equipos y servidores de la infraestructura informática.
- Ejecución intencionada de scripts que comprometan la seguridad y buena utilización de los recursos.
- Ejecutar las bases de datos de la Lotería de Boyacá para recolectar los datos contenidos en ella para uso externo de la empresa.
- Acceso no autorizado al software financiero y administrativo SINFAD y al software ABOX; o demás Software utilizados por la entidad.
- Realizar o modificar transacciones indebidas en el software financiero de la Lotería de Boyacá y/o sin la debida autorización.
- Ejecución de comandos SNMP al servidor.
- Utilizar cualquiera de los recursos informáticos de la Lotería de Boyacá para fines lucrativos diferentes a los contratos con la empresa.

Considerando lo anterior, las violaciones de las políticas de seguridad y privacidad por parte de funcionarios, contratistas pasantes o usuarios de los recursos tecnológicos darán lugar a la respectiva investigación de carácter disciplinario, penal, civil y fiscal.

5. PROPIEDAD INTELECTUAL

La Lotería de Boyacá podrá tener acceso en el momento que sea necesario a la información alojada en los equipos de cómputo, servidores, unidades lógicas entre otros, que son propiedad de la misma. Así mismo, podrá tener acceso a cualquier información generada y trasmitida por la red.

Todos los equipos de cómputo y servidores de la Lotería de Boyacá deberán pertenecer al dominio otorgado por el área de sistemas y sujetarse a las políticas de seguridad que estén establecidas actualmente, por lo tanto, cualquier software que este instalado en los equipos, deberá tener licencia y previa autorización por parte del equipo de sistemas para su correcto funcionamiento.

Se debe tener en cuenta que cualquier acción dentro del dominio se registra con el nombre de usuario individual, por lo cual los usuarios y claves del dominio son personales e intransferibles y cada uno es responsable de la utilización y del buen uso que les dé a los elementos informáticos, tales como uso de internet, correo, almacenamiento y transferencia de archivos, carpetas compartidas y utilización de las aplicaciones.

6. TRATAMIENTO DE DATOS PERSONALES

La Lotería de Boyacá dentro de la política de protección de datos personales en atención al objeto determinado por la Ley 1581 de 2012, el cual consiste en desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar la información que se haya recolectado sobre ella en la base de datos o archivos y los demás derechos, libertades y garantías constitucionales que se refiere el artículo 15 de la Constitución Política, establecerá el compromiso a cumplir frente a este criterio.

Con la política de protección de datos personales adoptada se debe administrar en pro al desarrollo de su objeto social, los criterios allí establecidos, es de obligatorio cumplimiento por parte de todos los funcionarios, contratistas, pasantes y terceros que obren en nombre de la Lotería de Boyacá en ejercicio de sus funciones y obligaciones contractuales.

7. REVISION DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

La Lotería de Boyacá debe revisar el plan de seguridad de la empresa a intervalos planificados, para asegurar su conveniencia, suficiencia y eficacia. Esta revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de cambios del mismo, incluido el plan de políticas de seguridad y privacidad de la información.

Como mínimo deberá revisarse 1 vez al año.

8. EVALUACION DEL DESEMPEÑO DEL PSPI

Con la intensión de conocer las etapas de cumplimiento de los objetivos del plan de seguridad y privacidad de la información, se mantendrán esquemas de seguimiento y medición al cumplimiento de aspectos de dicho documento para determinar y contextualizar una toma de decisiones de manera oportuna.

8.1. SEGUIMIENTO Y MEDICION

La Lotería de Boyacá definirá procedimientos que permitan tener un mayor control de las actividades de seguimiento y medición, como lo son:

- Definir y orientar actividades para la implementación de situaciones de eventos o incidentes de seguridad y privacidad de la información.
- Definir los esquemas de atención a los eventos e incidentes de seguridad de la información, en beneficio de prevenir y mitigar escenarios de impacto a la entidad.
- Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.
- Revisar las valoraciones de riesgo, asegurando que los niveles del mismo son comprendidos y aceptados.

9. MANTENIMIENTO Y MEJORA DEL PSPI

La Lotería de Boyacá con la visión de mantener y mejorar los aspectos del plan de seguridad y privacidad de la información, tomara en cuenta los resultados de la última revisión para verificar el estado del PSPI.

La Lotería de Boyacá:

- Implementara las mejoras identificadas en el PSPI
- Identificara e implementará acciones correctivas y preventivas que mitiguen situaciones de impacto.
- Asegurar que las mejoras cumplan con los objetivos y propósitos definidos por la Lotería de Boyacá.

RAFAEL LEONARDO ROJAS AZULA

Gerente General

Lotería de Boyacá

Revisó: German Ricardo Barbosa Granados
Aprobó: Melisa Jised Flórez Villalobos