LOTERÍA DEL HUILA
NIT. 800.244.699-7

PLAN DE SEGURIDAD

Y

PRIVACIDAD DE LA

INFORMACIÓN

ENERO 30 DE 2026

Carrera 4 No. 9-25
Edificio Diego de Ospina
Neiva, Huila

318 329 90 08 – 3183515317 – 3173686343
servicios@loteriadelhuila.com
www.loteriadelhuila.com

LOTERÍA DEL HUILA
NIT. 800.244.699-7

1. INTRODUCCION

Las Empresas reconocen la importancia de los sistemas en la Organización y los procesos productivos, de acuerdo a la gran revolución digital, y le da la importancia de tener su información adecuadamente identificada y protegida, bajo las relaciones de cumplimiento, comerciales y contractuales como los son acuerdos de confidencialidad y demás compromisos, que obligan a dar un tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia.

Los procesos que controlan los riesgos de seguridad de la información son aquellos que reducen las pérdidas y brindan protección, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

La Seguridad de la Información en las entidades permite conocer el estado de los activos de información ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio.

Por lo anterior se hace muy importante que las organizaciones cuenten con un plan de gestiónde riesgos para garantizar la continuidad del negocio.

2. OBJETIVO GENERAL

Desarrollar un plan de gestión de seguridad y privacidad que permita minimizar los riesgos de pérdida de activos de la información en la Empresa de Lotería y Juego de Apuestas Permanentes del Departamento del Huila, definiendo el plan de tratamiento de riesgos que hacen parte del Modelo de Seguridad y privacidad de la Información (MSPI).

De esta forma se busca que mediante el tratamiento de los riesgos se cree una herramienta con un enfoque sistemático que proporcione las pautas necesarias para desarrollar y fortalecer una adecuada gestión de los riesgos de seguridad de la información, identificación de riesgo y oportunidades, el análisis, la valoración y expedición de políticas así como el seguimiento y monitoreo permanente enfocado a su cumplimiento y mejoramiento.

2.1. OBJETIVOS ESPECIFICOS

- Realizar diagnóstico de la entidad por cada una de las dependencias, con el propósito de determinar el estado actual del nivel de seguridad y privacidad de la información.

- Determinar la factibilidad técnica, económica y operativa del Modelo de Seguridad y privacidad de la Información (MSPI), de acuerdo a la norma

ISO/IEC 27001:2013 (modelo internacional para la gestión de la seguridad de la información, proporciona un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI) con el fin de proporcionar confidencialidad, integridad y disponibilidad continuada de la información, así como cumplimiento legal).

- Elaborar el plan de seguridad y privacidad de la información, alineado con el propósito misional de cada una de las dependencias.

- Gestionar el riesgo asociado a la seguridad y privacidad de la información, mejorando los niveles de confianza a través su identificación, valoración, tratamiento y mitigación y monitorear y evaluar el desempeño del Modelo de Seguridad y privacidad de la Información (MSPI).

- Aplicar acciones de mejora continua, que garanticen el buen desempeño y efectividad del sistema y el avance al cumplimiento de las metas de Gobierno Digital.

- Fortalecer el sistema de gestión de riesgos de la Entidad incorporando controles y medidas de seguridad de la información que estén acordes al entorno operativo dela Entidad

- Reducir toda posibilidad de que una brecha o evento produzca determinado impacto en la información o cualquier otro activo de información asociado, a través de la gestión adecuada de los riesgos de la seguridad de la información.

3. ALCANCE

El Modelo de Seguridad y privacidad de la Información (MSPI) y su tratamiento, podrá será aplicada sobre cualquier proceso de la Empresa de Lotería y Juego de Apuestas Permanentes del Departamento del Huila, y cualquier sistema de información, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información , análisis y evaluación.

4. TERMINOS Y DEFINICIONES

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el control de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación,registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización.

Causa: Es todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

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

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Control: Medida que modifica el riesgo.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo, para determinar la magnitud y su impacto, aceptabilidad o tolerancia.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitar el riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

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

Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Monitoreo: Revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos.

Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Riesgo en la seguridad de la información: Potencial de que una amenaza causando así daño a la organización.

Reducción del riesgo: Acciones que se toman para disminuir la probabilidad de las consecuencias negativas, o ambas, asociadas con un riesgo.

5. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

En el marco del Modelo de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información –SGSI, se busca prevenir los efectos no deseados que se puedan presentar en cuanto a seguridad y privacidad de la información, por lo cual es importante controlar y establecer los riesgos de seguridad de la información.

De acuerdo a los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno Digital que viene impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información, Ley 1266 de 2008 Disposiciones generales de habeas data y se regula el manejo de la información, Ley 1273 de 2009 Código Penal, Ley Estatutaria 1581 de 2012, Protección de datos personales, Decreto 1074 de 2015 Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.

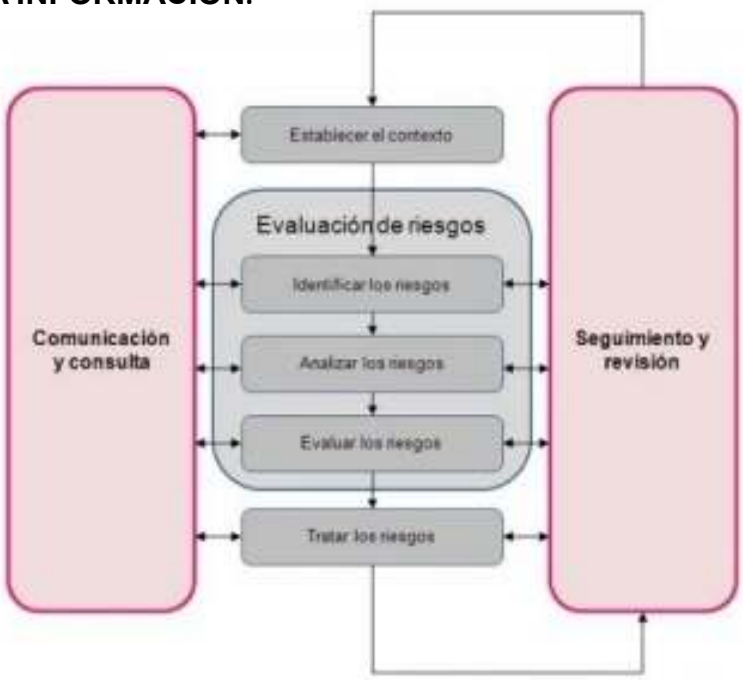
Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las empresas.

Una Empresa sin un plan de gestión de riesgos está expuesta a perder su información. Por esta razón es importante implementar planes para gestionar los riesgos que afectan a los sistemas de información, tecnologías de información y activos informáticos.

5.1 DEFINICION DEL RIESGO

La definición estandarizada de riesgo proviene de la Organización Internacional de Normalización (ISO), definiéndolo como “la posibilidad de que una amenaza determinada altere las vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la Entidad”.

5.2 VISION GENERAL PARA LA ADMINISTRACION DEL RIESGO DE SEGURIDAD DE LA INFORMACION.



Proceso para la administración del riesgo según los lineamientos generales de ISO 31000

5.3. IDENTIFICACION DEL RIESGO

- ✓ **Riesgo Estratégico:** Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

- ✓ **Riesgos de Imagen:** Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

- ✓ **Riesgos Operativos:** Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.

- ✓ **Riesgos Financieros:** Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

- ✓ **Riesgos de Cumplimiento:** Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y

en general con su compromiso ante la comunidad, de acuerdo con su misión.

- ✓ **Riesgos de Tecnología:** Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento dela misión.

Proceso para la evaluación del riesgo según los lineamientos generales de ISO 7001

5.4. ANALISIS DE VULNERABILIDADES

ANALISIS DE VULNERABILIDADES

Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios, y factores externos en la Empresa de Lotería y Juego de Apuestas Permanentes del Departamento del Huila se encontraron otras amenazas e impactos como los siguientes:

- La infraestructura física de la Entidad, es amplia, pero la red de cableado estructurado lleva más de 25 años sin mantenimiento y renovación del cableado estructurado, lo que genera pérdida de señal que afecta de forma directa el desempeño de las funciones.

- Los puntos de red eléctrica ubicados en cada oficina no son suficientes y se colocan nuevos según la necesidad. Creando un riego de posibles fallas eléctricas.

- A la red eléctrica le hace falta Balanceo de cargas, ya que en algunos casos se sobrecarga las UPS, por la cantidad de aparatos conectados.

- Bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de líquidos afectan los activos de información y de informática.

- En algunos papeles reutilizables se encuentra información personal o de la Entidad que debe ser reservada, identificándose la falta de confidencialidad y privacidad.

- Los usuarios de cada equipo de cómputo no realizan constantemente backup sobre sus archivos, existiendo un riesgo de pérdida de información en caso de un siniestro.

- La información en algunos casos es almacenada en memorias o discos duros portátiles personales, por ende, la información sale de la entidad.

- Falta de control frente al uso de dispositivos de almacenamiento externos, exponiendo a perder la información por virus no detectados o daños irreparables del hardware.

- Se identifica desconocimiento del tema de seguridad y privacidad de la información en la entidad, poniendo en riesgo la seguridad de la información.

- Los documentos físicos que se manejan en la entidad no se han digitalizado por lo tanto se encuentran expuestos a perdidas y daños físicos debido a que los sitios de almacenamiento en las oficinas no son los adecuados.

- No existe un sitio externo de almacenamiento de copias de seguridad de la información de la Entidad, aunque la base de datos y los aplicativos se encuentren alojados en la Nube.

- Los servidores de respaldo no cuentas con las especificaciones mínimas de enfriamiento y aislamiento de seguridad ya que comparten la misma temperatura de la Entidad y se encuentran expuestos a manipulación.

- No existe un plan de continuidad de negocio que permita reanudar las operaciones normales durante o después de interrupciones significativas a las operaciones de la Entidad. (en caso de incendio o desastre natural).

- Desconocimiento por parte de los usuarios del manejo de las páginas web, sede electrónica, correo electrónico y redes sociales.

6. MATRIZ DE VULNERABILIDADES Y MITIGACION DEL RIESGO

Como resultado de la etapa de evaluación del riesgo tendremos una lista ordenada de riesgos o una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos.

PROPUESTA DE SEGURIDAD

- Se debe realizar mantenimiento a la estructura física y a la red de cableado estructurado.

- Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias de cada oficina teniendo en cuanta la red de energía regulada y la red de energía normal.

- Socializar las políticas de seguridad y privacidad de la información con el personal de la Entidad, con el fin de concientizar a los usuarios de la importancia de reserva de la información de la Entidad.

- Crear un control frente a la utilización de dispositivos externos de almacenamiento conectados a los equipos de cómputo de la Entidad.

- Monitoreo permanente frente a los archivos o aplicaciones que se instalan en los pc de cada usuario para controlar posibles descargas o instalación de software dañino o virus que afecte los equipos y la información.

- Los documentos que contengan información de la empresa no reutilizarlos ya que puede salir datos o información de la Entidad.

- Crear un sitio de almacenamiento de backup en un sitio externo a la Entidad como respaldo a un desastre natural.

- Contar con un plan de almacenamiento de backup en la nube, como plan de contingencia en caso de desastre natural y pronta recuperación de la información.

- Aislar los servidores de contingencia en una ubicación donde permanezcan solos y con su respectiva temperatura que no permita el recalentamiento y peligro de la manipulación de personal no autorizado.

- Contar con un Plan alternativo que asegure la continuidad de la actividad del negocio de la Empresa de Lotería y Juego de apuestas Permanentes del Departamento del Huila en caso de desastres naturales o eventos graves.

- Capacitación continua sobre nuevas políticas y actualizaciones de tecnologías e ingresos a los diferentes links, redes sociales y la web.

La Empresa de Lotería y Juego de apuestas Permanentes del Departamento del Huila debe tener en cuenta que la Información requiere ser protegida y se debe trabajar sobre los tres pilares fundamentales:

Confidencialidad, Integridad y Disponibilidad.

Una de las principales características que debe poseer la entidad es buscar cómo establecer un Sistema de seguridad enfocado por procesos, resaltando la importancia que tienen las actividades de monitoreo y la correcta configuración para disminuir los riesgos y realizar tratamiento de las diferentes y constantes vulnerabilidades, para lo cual se deberán tener en cuenta los hallazgos y recomendaciones identificadas, cuyo propósito se encamine a mitigar los riesgos encontrados.

7. PLAN SEGURO PARA EL ALMACENAMIENTO DE COPIAS DE SEGURIDAD

Se debe tener en cuenta que la entidad puede sufrir un incidente que afecte su continuidad y dependiendo de la forma en que se gestionen dichos incidentes, las consecuencias pueden ser más o menos graves. Siempre teniendo en cuenta que la información requiere ser protegida y se debe trabajar sobre los tres pilares fundamentales: confidencialidad, integridad y disponibilidad.

8. PLAN DE CONTINUIDAD DEL NEGOCIO

- Diseñar un formato de chequeo de acuerdo a las necesidades de la organización que permita realizar auditorías periódicas con la finalidad de verificar que los objetivos de control, procesos y procedimientos se cumplan.

- Socializar con los directivos y oficina de las TIC la importancia del Plan de Continuidad de Negocio, para hacer frente a incidentes graves de seguridad en la Entidad, resumiendo de forma clara y sencilla cada una de las actividades a desarrollar dentro del plan.

- Diseñar estrategias para el proceso de recuperación teniendo en cuenta los tiempos de reacción e implementación de contingencias ante la realización de los eventos identificados.

- Adoptar una de las tres posiciones, que permita minimizar la ocurrencia o los efectos colaterales sobre la red, esto de acuerdo con los siguientes enfoques:

  - Detectar el riesgo
  - Plantear controles y efectuar las implementaciones respectivas.
  - Mitigar el riesgo.

- Diseñar un Plan de Contingencia teniendo en cuenta que la continuidad en el negocio dependerá de los riesgos y amenazas potenciales que serán tratados de acuerdo a lo siguiente:

  - Política de copia de seguridad de datos
  - Procedimientos de almacenamiento fuera de la Entidad
  - Procedimientos de gestión de emergencias, por desastre natural, por incendio o por inundaciones

9. IMPLEMENTACION DE POLITICAS DE SEGURIDAD PARA LA INFORMACION

El análisis permitió identificar que se desconocen y poco se cumplen las políticas de seguridad; por lo cual debe quedar integrado con el documento actual. Se recomienda entre otros tener en cuenta:

- ✓ Socialización y capacitación de temas de seguridad.
- ✓ Implementación de copia de seguridad externa.
- ✓ Contar con la seguridad física adecuada.
- ✓ Sistemas de respaldo para mantener soporte de la información en caso de eventualidades catastróficas.

10. PLAN DE CAPACITACION

Incluir dentro del plan de capacitaciones un espacio para integrar al personal encargado de manejar información y la seguridad de la misma para fortalecer aspectos como:

- ✓ Detectar los requerimientos tecnológicos
- ✓ Determinar objetivos de capacitación para personal
- ✓ Analizar los resultados de evaluaciones y monitoreo al sistema de seguridad.
- ✓ Elaborar un programa de capacitación en temas de ciberseguridad y políticas de seguridad de la información para todos los funcionarios de la entidad.
- ✓ Evaluar los resultados de cada actividad.

11. PLAN DE TRANSICION DE IPV4 A IPV6

Actualmente La Empresa de Lotería y Juego de Apuestas Permanentes del Departamento del Huila, se encuentra en proceso de la implementación de transición de las direcciones IPv4 existente actualmente por la IPv6, debido a que los equipos informáticos de la entidad soportan la nueva versión de IP en su gran mayoría y se encuentran trabajando con la base de datos y los aplicativos con un servicio de alojamiento en la Nube..

Para este proceso se realizó la recolección de la información necesaria, como el inventario de Hardware y Software que se realizó en cada una de las dependencias de la Entidad, de manera sucesiva se organiza la información de acuerdo con las plantillas sugeridas por el MINTIC en la “Guía de transición de IPv4 a IPv6 para Colombia”, con base en esto, se establece la información concerniente a equipos de cómputo, equipos de comunicación, servidores, aplicativos y equipos de impresión, siendo esta última sumada a las sugeridas en la guía, pues se ve la importancia del correcto funcionamiento de dichos equipos en la red de datos de la entidad.

12. MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.

- Decreto 612 de 4 de Abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.

- Decreto 1008 de 14 de Junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.

- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.

YHINA PAOLA LOMBANA LOPEZ
Gerente General

JAIR BALAGUERA VARGAS
Jefe de Oficina Administrativa y Financiera

DIEGO FERNANDO PASCUAS ARIAS
Jefe oficina Comercial y Operativa

CLAUDIA MIRYAN POLO ZULETA
P. U Talento Humano - Archivo y Almacén

MILLER ASTUDILLO MUÑOZ
P.U Sistemas y TICS

ORIGINAL FIRMADO