NUEVA LICORERA
· DE BOYACÁ E.I.C.E ·

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DIGITAL

NUEVA LICORERA
· DE BOYACÁ E.I.C.E ·

INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, busca la implementación de una política con orientación estratégica preventiva, al comprender el concepto de riesgo, así como se planean acciones que reduzcan las afectaciones a la **NUEVA LICORERA DE BOYACÁ** en caso de materialización.

La gestión de riesgos es la combinación de administrar el recurso humano, los procesos, los proyectos, las instalaciones y la implementación de mecanismos de prevención y mitigación de los riesgos identificados. Así mismo, la construcción de una cultura proactiva de conciencia y autocontrol frente al manejo del riesgo. Finalmente, la gestión integral de riesgos tiene como propósito reducir la probabilidad de ocurrencia y afectación en la continuidad de la operación de los procesos que utilicen los sistemas de información y la infraestructura tecnológica de la nueva Licorera de Boyacá.

El plan se elabora con base al Modelo de Seguridad y Privacidad de la Información - MSPI-emitida por Ministerio Tecnologías de la Información y las Comunicaciones - MinTIC con el fin de dar a conocer cómo se realizará la implementación y socialización del componente de Gobierno en línea en el Eje Temática de la Estrategia en Seguridad y Privacidad de la Información, el cual busca salvaguardar los datos y activos informáticos de la **NUEVA LICORERA DE BOYACÁ,** teniendo como finalidad principal garantizar la seguridad de la información.

GLOSARIO DE TERMINOS

- **Tolerancia al Riesgo:** Es el nivel de riesgo que la entidad está dispuesta a tolerar para que no afecte el desarrollo de los objetivos estratégicos.

- **Control:** Medida que se toma para modificar la exposición al riesgo, bien sea para disminuir la probabilidad de ocurrencia del evento o para disminuir su impacto.

- **Disponibilidad:** Capacidad de un componente o servicio para realizar su función requerida durante un periodo de tiempo.

- **Gestión Integral de Riesgos:** Es el proceso de identificación, valoración y control de los riesgos que amenazan el logro de los objetivos de la entidad.

- **Identificación de riesgos:** Es el proceso de encontrar, reconocer y definir los escenarios de riesgo, sus causas y sus potenciales consecuencias.

- **Proceso:** Grupo de actividades relacionadas de manera lógica que, cuando se llevan a cabo, utilizan los recursos de la entidad para lograr resultados definitivos o transformar elementos de entrada, a través de una serie de actividades, en un producto o servicio.

- **Responsable del Riesgo:** Persona o entidad que tiene la responsabilidad y autoridad para gestionar el riesgo a través de la implementación de los planes de mitigación.

- **Riesgo:** Es la exposición a una situación donde hay una posibilidad de sufrir un daño o de estar en peligro. **Es esa vulnerabilidad y amenaza a que ocurra un evento y sus efectos sean negativos y que los activos puedan verse afectados por él.**

- **Riesgo inherente:** Es el riesgo intrínseco de cada actividad, sin tener en cuenta los controles que de éste se hagan a su interior. Este riesgo surge de la exposición que se tenga a la actividad en particular y de la probabilidad que un impacto negativo afecte la rentabilidad, el capital de la compañía, y sus procesos.

- **Riesgo residual:** Es aquel riesgo que subsiste, después de haber implementado controles. Es importante advertir que el nivel de riesgo al que está sometido una entidad nunca puede erradicarse. Por ello, se debe buscar

un equilibrio entre el nivel de recursos y mecanismos que es preciso dedicar para minimizar o mitigar estos riesgos y un cierto nivel de confianza que se puede considerar suficiente (nivel de riesgo aceptable). El riesgo residual puede verse como aquello que separa a la entidad de la seguridad absoluta.

- **Seguridad de la Información:** Conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.
- **Tratamiento del riesgo (Plan de Mitigación):** Selección y aplicación de medidas, con el fin de poder modificar la magnitud del riesgo, para evitar de este modo los daños intrínsecos de materializarse.

- **GSIT:** Gestión de Servicios de Infraestructura Tecnológica.

- **Impacto:** Es el resultado de la materialización de un evento.

- **Probabilidad:** Se refiere a la posibilidad de ocurrencia de un riesgo potencial.

- **Usuario:** Persona que utiliza los servicios diarios.

OBJETIVO GENERAL

Establecer los lineamientos sobre las acciones que se deben adelantar en la Nueva Licorera de Boyacá, encaminadas a implementar un plan de tratamiento de riesgos con el fin de disminuir la probabilidad de ocurrencia y el impacto de todas aquellas acciones y situaciones que puedan interferir con la continuidad de la operación de la infraestructura tecnológica y los sistemas de información que afecten el funcionamiento de los procesos de la entidad.

OBJETIVOS ESPECIFICOS

- Determinar alcance del plan de tratamiento de riesgos de seguridad y privacidad de la información.
- Realizar el diagnostico y levantamiento del inventario de activos de información a proteger en la Nueva Licorera de Boyacá-NLB
- Diseñar la matriz de riesgos asociados a la infraestructura tecnológica y sistemas de información.
- Garantizar la confidencialidad e integridad de los activos de información de la entidad minimizando el riesgo que se pueda generar por la fuga o pérdida de alguna credencial de acceso.
- Levantamiento de el inventario de la información clasificada y reservada de la Nueva Licorera de Boyacá.

ALCANCE

El presente Plan de Tratamiento aplica para toda la Nueva Licorera de Boyacá, funcionarios, contratistas y terceros, que tengan acceso, usen, produzcan o manejen información de los procesos estratégicos, misionales, de apoyo y de evaluación, de la Entidad.

DECLARACIÓN

En este documento se encuentran los lineamientos que aseguran una actuación adecuada para alcanzar un alto nivel en cuanto a seguridad de la información en la Nueva Licorera de Boyacá. La información es un activo importante para la entidad, tiene un alto valor para la misma, por esto mismo la unidad ha definido las directrices de seguridad para los Activos de Información, por medio de las cuales se deben orientar todas las acciones a seguir.

Estas directrices hacen parte del marco de POLÍTICAS Y SEGURIDAD DE INFORMACIÓN y se tiene en cuenta algunas definiciones y conceptos de la NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27002, en forma generalizada.
Por lo anterior, se busca minimizar los riesgos asociados a los activos de información, asegurar la continuidad de la operación en la Nueva Licorera de Boyacá, y ayudar en el cumplimiento de los objetivos misionales.

1.1. Acuerdo de confidencialidad:

Todos los Usuarios que administran, leen, modifican o crean información en la Nueva Licorera de Boyacá, deben firmar un acuerdo de confidencialidad o de no divulgación como parte de sus términos y condiciones iníciales de empleo. Consignados en la

cláusula sexta obligaciones del contratista numeral 10. Confidencialidad. (todos trabajadores de la NLB -TIENE LA OBLIGACION DE CUMPLIMIENTO DE CLAUSULA DE CONFIDENCIALIDAD) Esta directriz también incluye a contratistas, personal ocasional y los Usuarios externos no contemplados en un contrato formalizado.

ROLES Y RESPONSABILIDADES

Control Interno: o quien haga sus veces se enmarca en cinco funciones: valoración del riesgo, acompañamiento y asesoría, evaluación y seguimiento, fomento de la cultura del **control** y relación con los entes externos

Jefe de planeación:

- Aprobar las modificaciones y nueva versión de los documentos y elementos del Sistema Integrado de Gestión SG.
- Asegurar que se establezcan, implementen y mantengan los procesos necesarios para SG.
- Asegurar que se promueva la toma de conciencia de los requisitos de los usuarios en todos los niveles de la Institución.
- Informar a la alta dirección sobre el desempeño de los Sistema de Gestión -SG- y de cualquier necesidad de mejora.
- Sugerir actualizaciones al marco normativo de seguridad de la información de la empresa cuando un requerimiento del negocio, contractual o del proceso genere la necesidad.
- Liderar los proyectos y planes de mejoramiento de seguridad de la información asociados a la gestión de riesgos sobre la información de su proceso.
- Participar en las decisiones de seguridad de la información.

- Asegurar el establecimiento, implementación, operación, seguimiento y mejoramiento del SG en sus procesos.
- Garantizar los recursos humanos para la ejecución de los planes de auditorías al SG.
- Aprobar la identificación, evaluación y tratamiento de riesgos sobre los activos de sus procesos.
- Asegurar el seguimiento de la gestión de riesgos asociados a los activos de sus procesos.
- Aprobar la implementación, comunicar y asegurar la aplicación de los controles/ medidas administrativas para tratar los riesgos sobre la información de sus procesos.
- Hacer seguimiento al manejo de Anomalías del SG.
- Aprobar la identificación, valoración y clasificación de la información en sus procesos.
- Determinar la información que hará parte del alcance del SG.

Líder de cada proceso: es aquel con capacidad para influir y persuadir, para que todos los miembros del equipo ejerzan su desempeño y logren los mejores resultados por sus propias razones (las de los individuos), y de esta manera **ejerce** el poder.

Encargado de seguridad de la información: Persona delegada cuyas funciones principales son asesorar en materia de seguridad de la información a la Nueva Licorera de Boyacá, y supervisar el cumplimiento de la presente Política.

Usuarios: personas que intervienen directamente sobre los diferentes procesos de riesgos digitales y que estén involucrados en el sistema de información de la empresa NLB;

PLAN DE SEGURIDAD PARA LA GESTION DE RIESGOS.

Los riesgos de seguridad digital se basan en la afectación de 3 criterios en un activo o un grupo de activos dentro del proceso: “Integridad, confidencialidad o disponibilidad”.

La Nueva Licorera de Boyacá NLB, se compromete a gestionar los riesgos, identificando y administrando los eventos potenciales que pueden afectar la plataforma estratégica, los objetivos institucionales y procesos de la NLB. Para la adecuada gestión integral del riesgo en la Nueva Licorera de Boyacá, se presenta los Siguientes lineamientos:

1. Se adoptará el proceso para la administración del riesgo, para gestionar los riesgos de la Nueva Licorera de Boyacá NLB, a través del análisis del contexto, entendido como el entorno externo e interno, y la valoración de los mismos, es decir, su identificación, análisis y evaluación, y su posterior tratamiento, todo esto manteniendo comunicación y consulta constante y permanente monitoreo y revisión, para evitar así su materialización.

Proceso para la Administración del Riesgo

2. Asegurar los recursos necesarios para ayudar a los responsables a gestionar y tratar los riesgos.
3. Los riesgos que se gestionan en la Nueva Licorera de Boyacá son los SGuientes:

    a) **Riesgos Estratégicos:** Probabilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.
    b) **Riesgos Genréciales:** Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
    c) **Riesgos operativos:** Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
    d) **Riesgos financieros:** Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso

financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.

e) **Riesgos tecnológicos:** Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.

f) **Riesgos de cumplimiento:** Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones

g) contractuales.

h) **Riesgo de imagen o reputacional:** posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización, ante sus clientes y partes interesadas.

i) **Riesgos de corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado**.**

j) **Riesgos de seguridad digital:** Posibilidad Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

4. Se deben identificar los activos de información por cada proceso (Ver procedimiento de activos de información).

5. Se deben identificar los responsables de los activos. (formato registro de activos de información)

6. Se deben clasificar los activos. (ver procedimientos activos de información)

7. Se deben identificar las vulnerabilidades de los activos. (Procedimiento Para Abordar Riesgos Del SG - Matriz Integral De Riesgos DE-SG-PR-04)

8. Se deben identificar las amenazas de los activos. (Procedimiento Para Abordar Riesgos Del SG - Matriz Integral De Riesgos DE-SG-PR-04)

9. Se deben identificar los riesgos de los activos. (Procedimiento Para Abordar Riesgos Del SG - Matriz Integral De Riesgos DE-SG-PR-04)

10. Se debe realizar una descripción de los riesgos. (Procedimiento Para Abordar Riesgos Del SG - Matriz Integral de Riesgos DE-SG-PR-04)

11. Se debe revisar la probabilidad y el impacto de ocurrencia de los riesgos. (Procedimiento Para Abordar Riesgos Del SG - Matriz Integral de Riesgos DE-SG-PR-04)

12. Se debe calcular el riesgo inherente. (Procedimiento Para Abordar Riesgos Del SG - Matriz Integral de Riesgos DE-SG-PR-04)

13. Se deben aplicar los controles a los riesgos identificados. (Procedimiento Para Abordar Riesgos Del SG - Matriz Integral de Riesgos DE-SG-PR-04)

14. Los controles deben tener una frecuencia de aplicación. (Procedimiento Para Abordar Riesgos Del SG - Matriz Integral de Riesgos DE-SG-PR-04)

15. La tolerancia es el nivel del riesgo que la entidad puede o está dispuesta a soportar, que corresponden a los riesgos que se encuentren en zona residual Baja y los que se encuentran en otra zona se trataran de acuerdo con los lineamientos

establecidos en el procedimiento (Procedimiento Para Abordar Riesgos Del SG de la Nueva Licorera de Boyacá.

16. La entidad revisará y actualizará la política de Gestión de Riesgos de acuerdo con los cambios del entorno, las nuevas metodologías y los resultados de los indicadores de gestión asociados a la materialización de riesgos definidos.

17. Los riesgos identificados en la entidad deberán ser monitoreados permanentemente, para asegurar que los controles sean eficaces y eficientes, y obtener información para mejorar la evaluación y gestión de los riesgos e identificar la materialización oportuna de los riesgos. (Procedimiento Para Abordar Riesgos Del SG)

18. Los niveles de responsabilidad sobre periodicidad de seguimiento y evaluación de los riesgos se llevarán a cabo de acuerdo procedimiento de (Procedimiento Para Abordar Riesgos Del SG - Matriz Integral de Riesgos DE-SG-PR-04).

19. Comunicar interna y externamente, los resultados de la gestión del riesgo desarrollada institucionalmente, los riesgos priorizados de acuerdo con los lineamientos establecidos en el procedimiento de (Procedimiento Para Abordar Riesgos Del SG - DE-SG-PR-04).

20. Las opciones del tratamiento a los riesgos que se evalúan en la entidad son:

    a. **Evitar el riesgo:** Se logra cuando al interior de los procesos se genera cambios sustanciales por rediseño, eliminación o cancelación de una actividad o conjunto de actividades que causan el riesgo, resultado de unos adecuados controles y acciones emprendidas. Por ejemplo: el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

b. **Reducir el riesgo:** Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Por ejemplo: a través de la optimización de los procedimientos y la implementación de controles.
c. **Compartir el riesgo:** Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones o dependencias, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización.
d. **Asumir el riesgo**: Después de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, el líder del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo. No aplica para los riesgos de corrupción, estos siempre deben conducir a un plan de acción o de tratamiento para mitigarlo.

Riesgos de Seguridad y Privacidad de la Información Digital.

Los riesgos en seguridad y privacidad de la Información digital están asociados con el potencial de que las amenazas exploten la vulnerabilidad de un activo de información o grupo de activos de información y, por lo tanto, causen daños a la empresa. Teniendo en cuenta lo anterior la Nueva Licorera de Boyacá estable los criterios de Impacto para riesgos de Seguridad y Privacidad de la Información Digital que permitirán llevar a cabo el tratamiento de los mismos en caso de que llegasen a ocurrir.

Criterios de Impacto Para Riesgos de Seguridad Digital			
Nivel	**Consecuencias Cuantitativa**	**Consecuencias Cualitativa**	**Valor**
INSGNIFICANTE	* Afectación en un valor menor o igual al 1% de la población. * Afectación en un valor menor o igual al 1% del presupuesto anual de la empresa. * No hay afectación medioambiental.	* Sin afectación de la integridad. * Sin afectación de la disponibilidad. * Sin afectación de la confidencialidad.	1
MENOR	* Afectación en un valor mayor al 1% y menor o igual al 10% de la población. * Afectación en un valor mayor al 1% y menor o igual al 10% del presupuesto de seguridad de la información en la empresa. * Afectación leve del medio ambiente que requiere de 1 a 3 meses de recuperación.	* Afectación leve de la integridad. * Afectación leve de la disponibilidad. * Afectación leve de la confidencialidad.	2
MODERADO	* Afectación en un valor mayor al 10% y menor o igual al 20% de la población. * Afectación en un valor mayor al 10% y menor o igual al 20% del presupuesto de seguridad de la información en la empresa. * Afectación leve del medio ambiente que requiere de 4 meses a 1 año de recuperación.	* Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. * Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. * Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y Terceros.	3

MAYOR	* Afectación en un valor mayor al 20% y menor o igual al 50% de la población. * Afectación en un valor mayor al 20% y menor o igual al 50% del presupuesto de seguridad de la información en la empresa. * Afectación importante del medio ambiente que requiere de 1 a 3 años de recuperación.	* Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. * Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. * Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.	4
CATASTRÓFICO	* Afectación en un valor superior al 50% de la población. * Afectación en un valor superior al 50% del presupuesto de seguridad de la información en la empresa. * Afectación muy grave del medio ambiente que requiere más de 3 años de recuperación.	* Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. * Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. * Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.	5

Acciones ante materialización de Riesgo

En caso de que en el desempeño actividad administrativa se materialicen riesgos identificados, en la matriz de riesgos institucionales, se deben aplicar y adoptar las Siguientes acciones por los responsables de cada proceso, dependiendo el tipo de riesgo materializado:

Tipo de Riesgo	Acción a aplicar o implementar	Responsable
RIESGO DE GESTIÓN Y SEGURIDAD DIGITAL (Zona Extrema, Alta y Moderada)	* Aplicar de manera inmediata el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o su restablecimiento, documentar en el Plan de mejoramiento. * Iniciar el análisis de causas y determinar acciones preventivas y de mejora y replantear los riesgos del proceso. * Actualizar el mapa de riesgos. * Informar al Proceso Estratégico sobre el hallazgo y las acciones tomadas.	Líder de proceso
	* Informar al líder del proceso sobre el hecho encontrado. * Informar a la segunda línea de defensa para dar inicio a las acciones correspondientes con el líder del proceso. * Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes. * Verificar que se tomaron las acciones pertinentes y se actualizó el mapa de riesgos.	Oficina de Control Interno de Gestión
RIESGO DE GESTIÓN Y SEGURIDAD DIGITAL	* Establecer acciones correctivas al interior de cada proceso y verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgos.	Líder de proceso
	* Informar al líder del proceso sobre el hecho encontrado. * Informar a la segunda línea de defensa para dar inicio a las acciones correspondientes con el líder del proceso. * Acompañar al líder del proceso en la revisión, análisis y toma de	Oficina de Control Interno de Gestión

	acciones correspondientes. * Verificar que se tomaron las acciones pertinentes y se actualizó el mapa de riesgos.	
RIESGO DE CORRUPCIÓN	* Informar al Proceso Estratégico sobre el hecho encontrado. * Una vez surtido el conducto regular establecido por la empresa y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), tramitar la denuncia ante la instancia de control correspondiente. * Identificar las acciones correctivas necesarias y documentarlas en el Plan de mejoramiento. * Efectuar el análisis de causas y determinar acciones preventivas, correctivas y de mejora. * Actualizar el mapa de riesgos.	Líder de proceso
	* Informar al Líder del proceso, quien analizará la situación y definirá las acciones correctivas a que haya lugar. * Una vez surtido el conducto regular establecido por la empresa y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente. * Informar a la segunda línea de defensa para dar inicio a las acciones correspondientes con el líder del proceso.	Oficina de Control Interno de Gestión

Control de Riesgos de Seguridad y Privacidad de la Información.

ACTIVOS	CONTROL	RESPONSABLE
HARDWARE	• Mantenimiento preventivos • Atención a Incidentes reportados •Verificación de Exposición del dispositivo a Humedad y Temperatura •Mantenimiento a Infraestructura de red de Datos •Mantenimiento a Infraestructura Eléctrica •Verificación del Dispositivo de Control de Energía (UPS)	Profesional Sistemas Tecnología
SOFTWARE	•Licenciamiento de Office •Instalación de Antivirus en Equipos de la NLB •Verificación de Ingreso a Bases de Datos de la NLB de Personal autorizado •Control de Instalación de aplicaciones •Control de Accesos y conexiones remostas a la red de la entidad •Realización de Copias de Seguridad	Profesional Sistemas Tecnología

CLASIFICACIÓN DE RIESGO

Para poder generar una sinergia en la comunicación y que en todas las áreas de la empresa se utilicen la misma terminología a la hora de identificar los riesgos en cada uno de los procesos, la NLB se permite entregar el Siguiente listado de clasificación de riesgos, para estandarizar el proceso de gestión, administración, identificación y evaluación de los tipos de riesgos:

- **Calidad:** riesgos relacionados con los atributos de calidad definidos en el MIPG
- **Contractual:** riesgos relacionados con los atrasos, incumplimientos y fallas en las etapasdel proceso contractual.
- **Operativos:** son los riesgos provenientes del funcionamiento y

operatividad de los procesos, de los sistemas de información, de la estructura de la empresa y la articulación entre las entidades.

- **Estratégicos:** riesgos asociados a la administración de la empresa, a la misión y el cumplimiento de los ejes estratégicos, la definición de las políticas, y las estrategias que responde a las necesidades de la NLB.
- **Imagen:** riesgos relacionados con la percepción y la confianza por parte de los grupos devalor frente a la empresa.
- **Financieros:** riesgos relacionados con el manejo de los recursos, la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes económicos de tesorería y el manejo de los bienes de la empresa.
- **Integración:** se refiere a riesgos relacionados a la integración de sistemas, áreas, entidades, etapas y elementos que se requieran coordinar para el desarrollo de estrategias, políticas, proyectos y/o planes.
- **Continuidad de negocio:** riesgos relacionados con la interrupción critica, parcial o total no deseada de las funciones de la empresa.
- **Recurso Humano:** este riesgo se asocia a la cualificación, competencia y disponibilidad del personal requerido para el desarrollo de las funciones diarias de la NLB.
- **Tecnológicos:** riesgos relacionados con la capacidad tecnológica de la empresa (Hardware, Software, Redes) para satisfacer sus necesidades actuales, futuras y el cumplimiento de la misión y visión.
- **Comunicación:** riesgos relacionados con los canales, medios y oportunidades para informar durante las diferentes etapas del desarrollo y ejecución de un proyecto, plan, proceso, estrategia o actividad de la gestión institucional.
- **Cumplimiento y conformidad:** estos riesgos se asocian con los requisitos legales, contractuales, de ética pública y en general con nuestro compromiso ante la comunidad