NUEVA LICORERA
· DE BOYACÁ E.I.C.E ·

POLITICA DE SEGURIDAD DE LA INFORMACION

TABLA DE CONTENIDO

1. INTRODUCCION.

La adopción de políticas, normas y procedimientos de seguridad de la información obedece a una decisión estratégica de la Oficina de Sistemas Tecnologías de Información de la Nueva Licorera de Boyacá, con el fin de definir el SGSI, a través del análisis, diseño e implementación de los objetivos, requisitos de seguridad, procesos, procedimientos, planes, políticas, controles con formatos, la tecnología y estructura de la misma. En la actualidad la información para la Nueva Licorera de Boyacá, se reconoce como un activo supremamente valioso y en la medida que los sistemas de información apoyan cada vez más los procesos misionales y de apoyo, y en razón de lo anterior se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de la misma. Se ha definido que las políticas de seguridad de la información deben identificar responsabilidades y establecer los objetivos para una protección apropiada de los activos de información de la entidad, contando además con manuales para usuarios finales. La implementación de las políticas busca reducir el riesgo de que en forma accidental o intencional se divulgue, modifique, destruya o use en forma indebida la información de la entidad. Al mismo tiempo las políticas habilitan al área de Sistemas y Tecnologías de la Nueva Licorera de Boyacá y sus programas como responsables de dictar la normatividad de la gestión de seguridad de la información, y para orientar y mejorar la administración de seguridad de los activos de información. Finalmente, también contempla el proveer las bases para el seguimiento y monitoreo de la información producida y reservada al interior de en la entidad.

2. OBJETIVO

El objetivo principal de la presente Política es definir los principios y las reglas básicas para la gestión de la seguridad de la información con el único fin de lograr que en la NLB se garantice la seguridad de la información y se minimicen los riesgos que pueda perjudicar los procesos y procedimiento de la empresa.

El uso inapropiado expone a la Nueva Licorera de Boyacá y a las instituciones afiliadas a riesgos que pueden comprometer la integridad, confidencialidad y disponibilidad de la información.

3. ALCANCE

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de la Nueva Licorera de Boyacá y la ciudadanía en general.

4. GLOSARIO

Activo de información: Es el elemento de información que la entidad recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre 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.

Amenaza: Causa potencial de un incidente no deseado por el cual puede resultar dañado un sistema u organización. A modo de ejemplo, terremotos, inundaciones, sabotajes, amenazas de bombas, negligencias humanas, cortes eléctricos o fallas en los servidores, entre otras.

Análisis de riesgos de seguridad de la información: Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Base de datos: Conjunto organizado de datos personales que sea objeto de tratamiento. Para la aplicación de la presente política, debe distinguirse dos clases de bases de datos; las automatizadas, es decir, aquellas que se almacenan y administran a través de herramientas informáticas y las bases de datos manuales o archivos, donde la información se encuentra organizada o almacenada en medio físico y contienen información personal, tal como nombre, identificación, números de teléfono, correo electrónico, etc.,

Buena práctica: Actividades/Procesos/Modelos que se han usado con éxito por más de una organización durante cierto tiempo. ISO/Cobit/ITIL son ejemplos de buenas prácticas.

Cifrado: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información de la institución.

Confidencialidad: Es la propiedad de un documento o mensaje, que está autorizado para ser leído o entendido únicamente por las personas o entidades a las que va dirigido. Es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Dato Abierto: La Ley 1712 de 2014, menciona que son todos aquellos datos primarios 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.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. De acuerdo con la ley 1581 de 2012: Articulo 3: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Dato Privado: De acuerdo con la Sentencia T729 del 2002 de la corte constitucional, la información privada, será aquella que por versar sobre información personal o no, y
que, por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Es el caso de los libros de los comerciantes, de los documentos privados, de las historias clínicas o de la información extraída a partir de la inspección del domicilio.

Dato Público: 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.

Dato semiprivado: Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero, y crediticio de actividad comercial o de servicios a que se refiere el título IV de la ley 1266.

Datos 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.

Derecho de acceso: Son los permisos otorgados a un usuario, de acuerdo con sus funciones, para acceder a un determinado recurso o servicio de la Entidad.

Disponibilidad: Esta propiedad está destinada a garantizar el uso de los activos de información en el momento requerido.

Documento Reservado: Son aquellos a los cuales la Constitución y la ley le hayan otorgado este carácter. De acuerdo con la Ley 594 del 2000, “Ley general de archivo”, todas las personas tienen derecho a consultar los documentos de archivos públicos y a que se les expida copia de los mismos, siempre que dichos documentos no tengan carácter reservado conforme a la Constitución o a la ley. De acuerdo con la ley estatutaria 1437 de 2011, Código Contencioso Administrativo, Artículo 24:

Informaciones y documentos reservados, solo tendrán carácter reservado las informaciones y documentos expresamente sometidos a reserva por la
Constitución o la ley, y en especial:

- Los protegidos por el secreto comercial o industrial.
- Los relacionados con la defensa o seguridad nacionales.
- Los amparados por el secreto profesional.
- Los que involucren derechos a la privacidad e intimidad de las personas, incluidas en las hojas de vida, la historia laboral y los expedientes pensionales y demás registros de personal que obren en los archivos de las instituciones públicas o privadas, así como la historia clínica, salvo que sean solicitados por los propios interesados o por sus apoderados con facultad expresa para acceder a esa información.
- Los relativos a las condiciones financieras de las operaciones de crédito público y tesorería que realice la Nación, así como a los estudios técnicos de valoración de los activos de la Nación. Estos documentos e informaciones estarán sometidos a reserva por un término de seis (6) meses contados a partir de la realización de la respectiva operación.
- Los datos genéticos humanos.

Dominio: Conjunto de máquinas interconectadas pertenecientes a una red.

Incidente de seguridad: Es cualquier evento que tenga o pueda tener como resultado la interrupción de los servicios suministrados por un sistema informático y/o posibles pérdidas físicas, de activos o financieras. Se considera que un incidente es la materialización de la amenaza.

Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

Información pública clasificada: Como lo prescribe la Ley 1712 de 2014, 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.

Información pública reservada: En los términos de la Ley 1712 de 2014, 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.

Información de uso interno: Información de la Entidad que se encuentre en proceso de elaboración y no ha sido sometida al proceso de clasificación de la información.

Información personal: Información perteneciente al usuario y que ha sido almacenada en alguno de los activos de información de la Entidad.

Seguridad de la información: Es la propiedad que asegura que los recursos de un sistema de información sean utilizados de la manera correcta y que su acceso sólo sea posible a las personas que se encuentren autorizadas, preservando la Integridad, Confidencialidad y Disponibilidad de los activos de información.

Sistema informático: Plataforma tecnológica que puede incluir uno o más computadores, *software* relacionado, periféricos, terminales, procesos físicos, medios de transferencia de información y otros capaces de realizar procesamiento y/o transferencia de información.

Transferencia de datos: Tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera de Colombia, cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Vulnerabilidad: Cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños y producir pérdidas en la organización.

5. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas de seguridad de la información son el componente del SGS que marca el compromiso de la dirección con la seguridad de la información de la Nueva Licorera de Boyacá.

Las políticas de seguridad de la información, lejos de ser la descripción técnica de mecanismos o una expresión legal que involucre sanciones a conductas de los empleados, se alinea con la necesidad y razón de proteger, pues la política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos, así como un motor de intercambio y desarrollo en el ámbito de la participación individual en el negocio.

la política describe el uso apropiado de la información y de los sistemas de cómputo de la Nueva Licorera de Boyacá-NLB. Estas reglas se implementan para proteger al usuario (en adelante los empleados de la NLB y los usuarios de cualquier institución que use los sistemas de información de la empresa). El uso inapropiado expone a la Nueva Licorera de Boyacá y a las demás entidades

involucradas en los diversos procesos administrativos a riesgos que pueden comprometer la integridad, confidencialidad y disponibilidad de la información.

Estas políticas se encaminan hacia la preservación segura de todos los componentes sujetos de vulnerabilidad de la Nueva Licorera de Boyacá, como son:

Personas: orienta a los servidores públicos, funcionarios y contratistas de la Nueva Licorera de Boyacá que en el desarrollo de sus actividades laborales cotidianas puedan estar expuestos a riesgos extraordinarios en cuanto a su seguridad o pueda verse comprometida la seguridad de la Nueva Licorera de Boyacá.

Bienes: mediante la prevención y mitigación de los riesgos proporciona los lineamientos para proteger los recursos físicos y el software de la Nueva Licorera de Boyacá.

Información: conjunto de lineamientos de seguridad basados en la norma NTC-ISO-IEC 27001 que relaciona dominios y controles para minimizar los riesgos y amenazas que pueden afectar la integridad, confidencialidad o disponibilidad de la información en la Nueva Licorera de Boyacá.

6. NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance deberán dar cumplimiento un 100% de la política.

7. IMPORTANCIA DE INFORMACIÓN.

Los servicios de información y sistemas de cómputo de la Nueva Licorera de Boyacá son activos esenciales para el desarrollo de las diferentes actividades administrativas y de negocios, de igual manera se involucra entidades del Gobierno Departamental; en estos activos se exige que se instituyan y mantengan los niveles apropiados de seguridad de información. Es política de la Nueva Licorera de Boyacá-NLB que se tomen medidas apropiadas para proteger sus sistemas de cómputo

y los servicios de información contra la destrucción accidental o maliciosa, daño, modificación o revelación, y para mantener los niveles apropiados de confidencialidad, integridad y disponibilidad de tal información y/o de los servicios y sistemas de cómputo de la Empresa.

8. RESPONSABILIDAD CON LOS SERVICIOS Y SISTEMAS DE INFORMACION EN LA NUEVA LICORERA DE BOYACÁ.

Proteger, dar un buen uso y asumir como parte de nuestro trabajo la responsabilidad con relación a la información de la Empresa, considerada como un activo estratégico muy valioso de la NUEVALICORERA DE BOYACÁ-NLB, es una prioridad para todos quienes hacemos parte de la Empresa.

Para la NLB es un deber de sus funcionarios mantener niveles apropiados de seguridad de la información, mediante la definición y aplicación de políticas que impidan la destrucción de la misma de forma accidental o intencional. De igual manera, los controles establecidos pretenden evitar que la misma sea modificada o revelada a terceros, preservando su integridad, confiabilidad y disponibilidad para las personas, instituciones o áreas que la requieren en cumplimiento de las funciones asignadas por la empresa.

También es responsabilidad de la Empresa divulgar y explicar, de manera suficiente a todos los empleados, clientes y asociados, las normas establecidas para la seguridad de los recursos informáticos, con el fin de que cada uno de nuestros integrantes conozca la importancia de manejarlos adecuadamente, tengan plena conciencia de los riesgos que existen en relación con la información confidencial e identifiquen, con conocimiento de causa, ciertas restricciones y controles planteados en la política de uso de los servicios, equipos y de la información en los sistemas.

La presente "Política de uso apropiado de los Servicios de Información" hace una
descripción precisa de los aspectos básicos que los usuarios de recursos informáticos de la NLB deben conocer con el fin de que la tarea y administración de los mismos sea la adecuada y le garantice a la Empresa la protección, confidencialidad y fiabilidad de esta importante herramienta

de la gestión corporativa.

9. PRINCIPIOS DE LA POLITICA DE LA INFORMACION

La presente Política responde a las recomendaciones de las mejores prácticas de Seguridad de la Información recogidas en el Estándar Internacional ISO/IEC 27001, así como al cumplimiento de la legislación vigente en materia de protección de datos personales y de las normativas que, en el ámbito de la Seguridad de la Información, puedan afectar a la NLB

Los sistemas de cómputo de la NLB y toda la información en ellos son activos esenciales del negocio, y su uso inadecuado o abuso por parte de un usuario puede, a discreción de la NUEVA LICORERA DE BOYACÁ, exponer a ese usuario a la acción disciplinaria de conformidad con los procedimientos disciplinarios de la NLB. Dependiendo de la severidad del abuso del sistema, esto puede resultar en una advertencia de acuerdo con la normatividad de la Empresa para tal fin.

Los usuarios deben utilizar los sistemas y servicios de información de la NLB y los
dispositivos de comunicaciones de manera apropiada, legítima y consistente con sus obligaciones, con respeto hacia sus colegas y clientes. Estos dispositivos deben ser usados de conformidad con esta política y cualquier otra política, estándar o
procedimientos relevantes de la Nueva Licorera de Boyacá. Los usuarios (Empleados de planta, contratistas y visitantes) deben ser conscientes de que están en una entidad que representa y es propiedad de los Boyacenses, lo cual se ve en sus tratos con el mundo exterior cuando usan los sistemas de cómputo o los servicios de información de la NLB. Los usuarios deben ser conscientes de que sus acciones pueden afectar la imagen corporativa de la empresa, y pueden también involucrar contractualmente a la NLB e incurrir en obligaciones y responsabilidades por parte de la Empresa y del usuario.

A continuación, se establecen las 69 políticas de seguridad que soportan el SGSI de Nueva Licorera de Boyacá:

10. **SEGURIDAD LÓGICA.**

- ✓ **Política 1**. Longitud mínima de las claves de acceso debe ser de seis (6) caracteres y debe controlarse en el momento en que el usuario la construye o la selecciona.

- ✓ **Política 2.** Todas las palabras claves escogidas por el usuario para ingresar a los sistemas deben ser difíciles de identificar. En general, no se deben utilizar palabras de un diccionario, derivados del usuario-ID, series de caracteres comunes tales como "123456". Así mismo, no se deben emplear detalles personales como nombre del esposo, placas del carro, número del seguro y fecha de cumpleaños a menos que estén acompañadas por caracteres adicionales que no tengan ninguna relación. Las palabras claves escogidas por el usuario tampoco deben formar parte de una palabra. Por ejemplo, no se deben emplear nombres propios, sitios geográficos y jerga común.

- ✓ **Política 3**. Cambio periódico obligatorio de contraseña. El sistema debe obligar automáticamente a que todos los usuarios cambien sus palabras claves al menos una vez cada seis meses, de lo contrario el usuario por iniciativa propia debe hacerlo para todas y cada una de las aplicaciones y plataformas a que tenga acceso.

- ✓ **Política 4.** Cambio obligatorio de contraseña al acceder por primera vez el sistema. Las contraseñas inicialmente emitidas por un administrador de seguridad deben ser válidas solamente para la primera conexión del usuario, momento en el cual el usuario debe cambiar la palabra clave antes de realizar cualquier otro trabajo.

- ✓ **Política 5.** Utilización de contraseñas diferentes cuando se tiene acceso a varios sistemas

- ✓ **Política 6**. Sin importar las circunstancias, las contraseñas nunca deben ser compartidos o revelados a nadie más que al usuario autorizado. Hacerlo expone al usuario autorizado a responsabilizarse de acciones que otras personas hagan con su contraseña. Si los usuarios

necesitan compartir información permanente del computador, ellos deben usar correo electrónico, directorios públicos, en los servidores de red del área local u otros mecanismos.

- ✓ **Política 7.** Todas las contraseñas se deben cambiar tan pronto como se sospeche que han sido descubiertas o conocidas por otro.

- ✓ **Política 8.** Los usuarios son responsables de todas las actividades llevadas a cabo con su usuario y contraseña. De tal manera, los usuarios y contraseñas entregados por la Nueva Licorera de Boyacá son para el uso laboral legítimo como herramienta para el desarrollo de las actividades encomendadas, y por tanto son personales y su responsabilidad es intransferible.

- ✓ **Política 9.** Los computadores personales conectados a las redes LAN, WAN o internet de la Nueva Licorera de Boyacá una vez terminan su labor o esta debe ser interrumpida por alguna circunstancia, se debe salir de todas las aplicaciones a que haya ingresado y no exponer el computador a ingresos NO autorizados.

11. USO DE LOS SISTEMAS

- ✓ **Política 10.** Uso personal del computador y sistemas de comunicación. El computador de la Nueva Licorera de Boyacá y los sistemas de comunicación deben usarse solamente para asuntos de la Nueva Licorera de Boyacá.

- ✓ **Política 11.** Las Alteraciones o expansiones hechas a los Computadores dotados por la Nueva Licorera de Boyacá únicamente serán alterados o mejorados por el personal técnico de la Nueva Licorera de Boyacá o personal autorizado por la Nueva Licorera de Boyacá para tal fin.

- ✓ **Política 12.** Reporte de los Daños de Hardware – Software pertenecientes a la Nueva Licorera de Boyacá. Los funcionarios, contratistas, servidores públicos, Pasantes o judicantes deben reportar inmediatamente, por medio del formato (Solicitud de incidentes y diagnóstico código: GA-SAF-F-04) diseñado para tal fin, al profesional de sistemas, sobre cualquier daño o pérdida del equipo, software o información que tengan a su cuidado o custodia y sean propiedad de la Nueva Licorera de Boyacá.

- ✓ **Política 13.** Permiso para uso personal ocasional de los sistemas de la Nueva Licorera de Boyacá. Los sistemas de información de la Nueva Licorera de Boyacá deben usarse solamente para trabajos relacionados con las actividades de la misma, no obstante, el uso personal ocasional puede autorizarse por el superior o subgerente del área si:
    - no se consume más que una cantidad mínima de los recursos que podrían, en otra forma, usarse para asuntos del negocio,
    - (b) no interfiere con la productividad del trabajador, y
    - (c) no se apropia de ningún tipo de actividad comercial.

  Y en todo caso, debe hacerse en sus horas libres, y no en horas de trabajo de la Nueva Licorera de Boyacá.

- ✓ **Política 15.** Usos permitidos de información de la Nueva Licorera de Boyacá. La información de la Nueva Licorera de Boyacá debe usarse solamente con fines laborales expresamente autorizados por la administración.

- ✓ **Política 16.** Los privilegios de acceso a los sistemas de información se terminan cuando el funcionario se retira de la Nueva Licorera de Boyacá, el superior informará al profesional de sistemas para que el usuario sea desactivado a fin de evitar accesos no permitidos.

- ✓ **Política 17.** Cambios en la configuración del software instalado en los equipos de cómputo. No está permitido el cambio en la configuración estándar del software instalado en los

equipos de cómputo, tales como: - Configuraciones de red - Fondos de pantalla - Unidades de red - Configuraciones de dispositivos (impresoras, scanner)

12. **ADMINISTRACIÓN DE CONTROL DE ACCESO A LA INFORMACIÓN**

- ✓ **Política 18.** Controles de acceso a los computadores principales. Toda la información de los computadores principales (servidores) que sea sensible, crítica o valiosa debe tener controles de acceso al sistema para garantizar que no sea inapropiadamente descubierta, modificada, o borrada, además el acceso al lugar de almacenamiento está restringido al profesional de sistemas y a los miembros del comité directivo.

- ✓ **Política 19.** Capacidades del usuario para el acceso de archivos y su implicación en cuanto al uso. Los usuarios no deben leer, modificar, borrar, o copiar, de las carpetas públicas, un archivo que pertenezca a otro usuario, sin obtener primero permiso del propietario del archivo, a menos que el acceso general haya sido claramente proporcionado; sin responsabilidad alguna para los usuarios que ingresen y modifiquen, alteren, borren, o deterioren la información contenida en las carpetas públicas, pues es claro que la información bajo custodia del usuario no puede bajo ningún concepto estar en estas carpetas.

- ✓ **Política 20.** El número de la placa de inventario es la identificación única del computador dentro de la Nueva Licorera de Boyacá. Cada computador o sistema de comunicaciones debe tener una única identificación.

13. **ACTIVIDADES ADMINISTRATIVAS**

- ✓ **Política 21.** Revisión periódica y reevaluación de los privilegios de acceso del usuario. La Administración reevaluará el otorgamiento de los privilegios de acceso a los sistemas de todos y cada uno de los usuarios como máximo cada seis (6) meses y reportará los resultados al profesional de sistemas para las respectivas acciones correctivas.

- ✓ **Política 22.** Entrega de los usuarios y contraseñas a los funcionarios. Cuando el profesional de sistemas hace entrega a los funcionarios del usuario y contraseña otorgando el privilegio de acceso a los aplicativos, el funcionario acepta el acuerdo con la Nueva Licorera de Boyacá sobre la confidencialidad en el manejo de la información y el acatamiento de las normas de seguridad del sistema.

- ✓ **Política 23.** Reportes sobre cambios de tareas y responsabilidades. Las subgerencias deben informar oportunamente al profesional de sistemas, sobre todos los cambios de tareas y responsabilidades operativas o administrativas de los funcionarios, retiros e ingresos de nuevos funcionarios que dentro de sus labores desarrollen actividades relacionadas con sistemas de información, y del sistema de seguridad para actualizar, controlar y administrar los usuarios.

14. **VIRUS INFORMÁTICOS.**

- ✓ **Política 24.** Los funcionarios, contratistas, servidores públicos, Pasantes o judicantes deben reportar inmediatamente, haciendo uso de la herramienta que se encuentra en la intranet de la entidad pestaña ***Incidentes Tecnológicos*** y luego en **Centro de Soporte;** herramienta creada para el reporte de incidentes, al profesional de sistemas. Se prohíbe a los usuarios finales eliminar o ejecutar alguna acción o manipulación del sistema ya que puede llevar a ejecutar el virus y poner en riesgo los sistemas o equipos informáticos de la Nueva Licorera de Boyacá.

.

- ✓ **Política 25.** Los funcionarios de la Nueva Licorera de Boyacá no deben bajar o cargar Software de Internet en los sistemas corporativos por parte de terceras personas, hacerlo o permitir que terceras personas puedan bajar, cargar o instalar software de Internet en los sistemas de la Nueva Licorera de Boyacá. Esta prohibición es necesaria para proteger la red interna de, virus espías, troyanos, o virus secuestradores u otro software que puede dañar la información y los programas en producción.

- ✓ **Política 26** Es responsabilidad del usuario hacer la verificación de inexistencia de virus en medios de almacenamiento (como CD, DVD, memorias USB o discos duros externos) o programas o archivos ejecutables, en caso de contaminación debe solicitar el soporte a través de **intranet de la entidad pestaña** *Incidentes Tecnológicos* **y luego en** Centro de Soporte requerido(https://intranet.nlb.com.co/wp/incidentes/); y debe informar inmediatamente al Profesional de sistemas. Para prevenir la infección por virus en los computadores, los funcionarios de la Nueva Licorera de Boyacá no deb0en usar ningún software proporcionado externamente por persona u organización que no esté adecuadamente autorizada por la Nueva Licorera de Boyacá, además que únicamente el profesional de sistemas puede hacer la instalación de programas o descarga de archivos en los computadores de la Nueva Licorera de Boyacá. Los programas de terceros o provenientes de fuentes externas u obtenidos de internet, deben ser previamente examinados contra la presencia de virus, no pueden utilizarse en ningún computador personal (PC) o servidor de la red local (LAN) de la Nueva Licorera de Boyacá, a menos que hayan sido aprobado su uso por el profesional de sistemas; Si un virus es detectado debe notificarse por medio de **intranet de la entidad pestaña** *Incidentes Tecnológicos* **y luego en** Centro de Soporte requerido(https://intranet.nlb.com.co/wp/incidentes/); el Profesional de sistemas quien tomara medidas para evitar la propagación a todos los usuarios de la red para que se abstengan de bajar este software infectado a través de internet.

- ✓ **Política 27**. Todos los archivos magnéticos (programas, bases de datos, documentos de texto, etc.) deben ser descomprimidos antes de proceder a hacer una desinfección preventiva de virus informáticos para evitar la dificultad en la detección de virus en los programas o archivos comprimidos

- ✓ **Política 28.** El software original de los computadores personales debe preservarse en imágenes antes de iniciar su uso, estas copias deben almacenarse en un lugar seguro y confiable, no deben usarse para actividades comerciales ordinarias, deben reservarse para cuando se requiera restablecer el computador a su estado original de fábrica.

15. **OPERACIÓN DEL COMPUTADOR**

- ✓ **Política 29**. No se deben ingerir alimentos ni bebidas en cercanía de los equipos de cómputo de escritorio y portátiles, servidor, equipos activos de red, impresoras, monitores, teclados, escáneres, dispositivos señaladores y demás equipos electrónicos y de precisión.

- ✓ **Política 30**. Los usuarios no están autorizados para trasladar, desconectar o conectar equipos de cómputo sin la autorización y supervisión del profesional de sistemas A excepción de los equipos portátiles). Esta política mitiga el riesgo de daños en los equipos de cómputo por mala manipulación y facilita el control del inventario.

- ✓ **Política 31.** Ningún usuario está autorizado para modificar la configuración del Software Base (Sistemas Operativos, software controlador de dispositivos, software de ofimática, antivirus), ni la configuración del Setup de la máquina.

- ✓ **Política 32**. Todos los equipos de Cómputo se deben permanecer apagados fuera del horario laboral, con excepción de los Servidores y elementos activos de red. Durante las ausencias momentáneas el usuario debe activar el protector de pantalla con contraseña.

- ✓ **Política 33.** No se debe poner ningún elemento sobre los equipos de Cómputo, como por ejemplo Carpetas, materas, adornos, papeles, bolsas, y menos que se coloquen elementos que obstruyan los sistemas de ventilación.

- ✓ **Política 34.** Los equipos de Cómputo se deben conectar a las tomas (naranja) de corriente del Sistema Regulado de Energía (UPS). excepto las impresoras Láser que deben conectarse a las tomas de corriente Normal. No se debe conectar equipos eléctricos diferentes a los Equipos de Cómputo, al Sistema Regulado de energía (UPS).

- ✓ **Política 35**. Los usuarios deben apagar correctamente los computadores, cuidando de no dejar sesiones abiertas, o incurrir en apagado abrupto del computador con lo cual se deteriora el sistema operativo.

- ✓ **Política 36.** Los trabajos de mantenimiento deben ser coordinados con el profesional de sistemas y socializado por este a los usuarios.

16. **SEGURIDAD DE LOS DATOS**

- ✓ **Política 37**. La información se considera el recurso más importante de la Nueva Licorera de Boyacá, por tanto, es esencial que la Nueva Licorera de Boyacá proteja la información para garantizar su precisión, oportunidad y confiabilidad. La información deberá ser manejada adecuada y responsablemente y ser accesible sólo a las personas autorizadas, las normas, políticas y procedimientos Corporativos relacionados con los Sistemas de Información.

- ✓ **Política 38**. Sin excepción alguna, todo Software y su documentación generada y desarrollada por colaboradores, consultores, proveedores o contratistas para el beneficio y uso Corporativo, es propiedad exclusiva de la Nueva Licorera de Boyacá. Así como todos los derechos de propiedad legal sobre archivos fuente de aplicación y mensajes, son exclusivos de la Nueva Licorera de Boyacá.

- ✓ **Política 39.** Toda adquisición de software deberá tener su licencia por escrito a nombre de la Nueva Licorera de Boyacá, de la misma forma el profesional de sistemas eliminará el software y la información magnética que no sean de propiedad de la Nueva Licorera de Boyacá o que no cuente con las respectivas licencias de propiedad intelectual registradas y no tenga autorización específica para su almacenamiento y/o uso.

- ✓ **Política 40**. Dado que el software y la información son de la Nueva Licorera de Boyacá, ningún usuario está autorizado para copiar, transferir o divulgar software total o parcialmente.

- ✓ **Política 41**. Los funcionarios de la Nueva Licorera de Boyacá no deberán adquirir, poseer, comercializar o usar herramientas de hardware o software que pudieran emplearse para evaluar o comprometer la seguridad de los sistemas de información. Si la Nueva Licorera de Boyacá considera utilizar este tipo de herramientas tecnológicas para la evaluación de la seguridad de los sistemas, deberán ejecutarse en el ambiente controlado.

- ✓ **Política 42**. En cumplimiento de las normas vigentes de Manejo de la información confidencial, toda información confidencial o de propiedad de terceros, que se ha confiado a la Nueva Licorera de Boyacá, se tratará y protegerá de igual forma que la información confidencial interna.

- ✓ **Política 43.** El software de la Nueva Licorera de Boyacá, su documentación y en general la información interna, no deben ser enviados o trasladados a sitios que no son de la Nueva Licorera de Boyacá, sin que la alta dirección no lo ordene y asuma la responsabilidad de este traslado.

- ✓ **Política 44.** La alta dirección se reserva el derecho de examinar todos los datos guardados o transmitidos en sus sistemas, como las computadoras y los sistemas de comunicaciones de la Nueva Licorera de Boyacá.

- ✓ **Política 45** Revelar la información que exija la ley, las instituciones de control del estado o la que ordene la alta Dirección de la Nueva Licorera de Boyacá. Los usuarios deben permitir que toda la información que este en su poder dentro de la Nueva Licorera de Boyacá, pueda ser conocida por instrucciones de ley y a discreción de la Nueva Licorera de Boyacá, con el acompañamiento siempre del Profesional de Sistemas.

- ✓ **Política 46**. La Nueva Licorera de Boyacá no revelará los nombres, títulos, números de teléfono, localización u otra información particular de sus colaboradores a menos que sea requerido para propósitos del objeto social de la Nueva Licorera de Boyacá. Se harán

excepciones cuando dicha revelación sea exigida por entidad del gobierno, exigencia legal o por consentimiento previo de los involucrados.

✓ **Política 47.** La información sensible y personal recolectada de los clientes, tal como número telefónico y dirección, se debe usar para propósitos internos de la Nueva Licorera de Boyacá y se deberá entregar a terceros si el cliente ha proporcionado su consentimiento anteriormente por escrito, y por solicitud escrita de entidades gubernamentales o entes de control.

17. **CONFIDENCIALIDAD DE LOS DATOS**

✓ **Política 48.** Confidencialidad de la Información. Toda la información que tenga carácter confidencial, en los términos establecidos en la ley, deberá enmarcarse en lo establecido en la legislación nacional vigente.

✓ **Política 49.** Los funcionarios deben obtener autorización de aprobación específica por parte de la alta dirección, para destruir o disponer de la información que es potencialmente importante para la Nueva Licorera de Boyacá. Una destrucción no autorizada de los registros o información de la Nueva Licorera de Boyacá puede conllevar a acciones disciplinarias incluyendo la terminación del contrato y procesos legales a que haya lugar. Los registros y la información se deben conservar en caso de: que las normas nacionales lo determinen, o que se proyecte su necesidad en el futuro, o en caso de que puedan ser necesitados como pruebas en investigaciones de organismos de control o entidades del estado.

✓ **Política 50.** Toda información parcial o incompleta, obsoleta o en desuso debe ser suprimida y no puede ser publicada interna o externamente; a menos que esté acompañada de una explicación que describa la naturaleza de dicha información como informes preliminares, resultados sujetos a validación, etc.

- ✓ **Política 51** Toda información al público debe ser validada o autorizada por la alta dirección o por los funcionarios autorizados para hacerlo.

- ✓ **Política 52.** Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación y cómputo de la Nueva Licorera de Boyacá son restringidas, de tal forma que no deben ser conocidas por clientes o personas ajenas a la organización.

18. **SEGURIDAD EN COMUNICACIONES**

- ✓ **Política 53.** La conexión a Internet requiere de implementar mecanismos adicionales de control de acceso este procedimiento será realizado por el profesional de sistemas.

- ✓ **Política 54.** No están permitidas las conexiones remotas a computadores de la entidad a través de herramientas de conexión a escritorio remoto o similares

19. **SISTEMAS DE CORREO ELECTRÓNICO**

- ✓ **Política 55.** Asignación y responsabilidades sobre el uso del correo Electrónico:

- Los funcionarios y contratistas de la Nueva Licorera de Boyacá s deben emplear las direcciones de correo electrónico corporativas asignadas para atender los asuntos de la Entidad.
- Todos los funcionarios y contratistas de la entidad, aceptan la responsabilidad del buen manejo de la cuenta de correo institucional.
- Cada usuario debe depurar continuamente su buzón de correo con el fin de mantener espacio disponible para la recepción de nuevos mensajes.
- Cada usuario es responsable de la información enviada y reenviada desde su cuenta de correo.
- No está permitido el envío de correos masivos.

- No está permitido usar una Cuenta de Correo Electrónico diferente a la asignada

✓ **Política 56.** Autorización para Leer Correo Electrónico de Otros Colaboradores Política: Cuando el director de Dependencia y el director de Gestión Humana estén colectivamente de acuerdo, los mensajes de correo electrónico viajando a través de los sistemas de la Nueva Licorera de Boyacá pueden ser monitoreados para cumplir con políticas internas, por sospechar la actividad criminal, y otras razones de sistemas de gerencia. A menos de que este trabajo sea específicamente asignado por los gerentes, el monitoreo de los mensajes de correo electrónico está prohibido por cualquier otro trabajador.

✓ **Política 57.** Restringir el Contenido del mensaje en el Sistema de Información de la Nueva Licorera de Boyacá. Los funcionarios tienen prohibido enviar o remitir por medio del sistema de información de la Nueva Licorera de Boyacá, cualquier mensaje que se pueda considerar difamatorio, hostil o explícitamente sexual, de igual manera, también está prohibido enviar o remitir mensajes o imágenes que puedan ofender las creencias de raza, género, nacionalidad, orientación sexual, religión, creencias políticas o discapacidad.

✓ **Política 58**. Los Mensajes de Correo Electrónico son Registros de la Nueva Licorera de Boyacá y en tal sentido, este sistema será usado únicamente para propósitos de trabajo. y la Nueva Licorera de Boyacá se reserva el derecho de acceder y revelar todos los mensajes enviados por medio del sistema de correo electrónico para cualquier propósito.

20. **COPIAS DE SEGURIDAD Y CUSTODIA DE LA INFORMACIÓN.**

✓ **Política 59**. Cada usuario es responsable por la custodia de la información sensible que genera y tiene almacenada en su computador.

✓ **Política 60**. Cada usuario es responsable por la correcta organización y clasificación en carpetas y subcarpetas, de los archivos en medios magnéticos que tiene a su cargo. No se deben guardar estos archivos en el escritorio de Windows, ni en ninguna de las carpetas

estándar de Windows identificadas con los nombres de imágenes, documentos, música, video, etc. Estos archivos deben ser almacenados en las carpetas y subcarpetas creadas por cada usuario en el directorio raíz del disco duro de los equipos asignados, así como tampoco se deben guardar en los computadores de la entidad archivos personales.

- ✓ **Política 61**. Las Copias de respaldo de la información almacenada en los computadores de la Nueva Licorera de Boyacá son responsabilidad de cada funcionario, el profesional de sistemas es responsable de las copias de seguridad de la información de las bases de datos y programas de la Nueva Licorera de Boyacá, así como de la información que los usuarios solicitan sea integrada a estas copias de seguridad.

- ✓ **Política 62**. La información sensible relacionada con las operaciones de la Nueva Licorera de Boyacá, no debe ser almacenada en sitios públicos gratis en la nube como los repositorios de información (Dropbox, box, Google Drive, Ondrive, etc), debido a que esta información podría estar expuesta a accesos no autorizados. Solo pueden ser utilizados los sitios públicos corporativos en la nube que han sido autorizados previamente

- ✓ **Política 63.** Las copias de seguridad de la información tanto de los usuarios como la de los servidores, deben estar encriptadas para evitar el riesgo de accesos no autorizados a esta información.

21. **SEGURIDAD FÍSICA**

- ✓ **Política 64.** El acceso físico a cada oficina, cuarto de computadores y área de trabajo que contiene información sensible, debe ser físicamente restringido y registrado o autorizado por la subgerencia Administrativa y financiera

- ✓ **Política 65.** El acceso a las oficinas de la Nueva Licorera de Boyacá por parte de visitantes u otras personas debe estar controlada por los guardas o recepcionistas. A los visitantes no se les debe permitir el acceso no controlado a ninguna instalación de la Nueva Licorera de Boyacá.

22. **REGISTRO DE ACCESO A LAS INSTALACIONES.**

Política 69. Para facilitar la evacuación, sustentar investigaciones, y demás indicadas por entidades de control, del gobierno o de la alta dirección, los guardas deben mantener registros del personal actual y el que ingresó previamente a las instalaciones de la Nueva Licorera de Boyacá. Esta información debe guardarse.