PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
NUEVA LICORERA DE BOYACÁ.

Un Sistema de Seguridad Informática es un conjunto de elementos administrativos, técnicos y personal que de manera interrelacionada garantizan niveles de seguridad informática en correspondencia con la importancia de los bienes a proteger y los riesgos estimados.

El Plan de Seguridad Informática es la expresión gráfica del Sistema de Seguridad Informática diseñado y constituye el documento básico que establece los principios organizativos y funcionales de la actividad de Seguridad Informática en una Entidad y recoge claramente las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático, así como las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas que gravitan sobre el mismo.

La política de seguridad Es un componente del SGS que marca el compromiso de la dirección con la seguridad de la Información de la Nueva Licorera de Boyacá, establece el canal formal de actuación del personal, hacia el desarrollo de buenas prácticas y dicta lineamientos para la seguridad de la entidad.

La política de seguridad de la información, lejos de ser una descripción técnica de mecanismos o una expresión legal que involucre sanciones a conductas de los empleados, se alinea con la necesidad de proteger los elementos, 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.

Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.

1. OBJETIVOS.

Establecer las normativas y políticas para el uso, control y administración de las Tecnología de Información y Comunicaciones que deben conocer y cumplir todos los funcionarios, definiendo los mecanismos y todas las medidas necesarias por parte de la NLB, tanto técnica, lógica, física, legal y ambiental para la protección de los activos de información, los recursos y la tecnología de la entidad, con el propósito de evitar accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir de forma intencional o accidental, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Fortalecer la cultura de seguridad de la información en funcionarios, terceros y clientes de NUEVA LICORERA DE BOYACA, mediante la definición de una estrategia de uso y apropiación de la política.

1.2. OBJETIVOS ESPECÍFICOS

La NUEVA LICORERA DE BOYACÁ, para asegurar el direccionamiento estratégico de la Entidad, establece la compatibilidad de la política y de los objetivos de seguridad de la información, estos últimos correspondientes a:

- Mitigar los riesgos de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Apoyar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios y clientes externos
- Garantizar la continuidad del servicio frente a incidentes.

2. ALCANCE

La presente política será aplicable a todos: Servidores públicos, funcionarios, contratistas (persona natural vinculada a la Entidad mediante contrato de prestación de servicios y apoyo a la gestión), pasantes y/o judicantes, proveedores, visitantes y terceros que hacen parte del sistema de la Nueva Licorera de Boyacá que, de una u otra forma se relacione con sistemas de información o utilizan la Infraestructura Tecnológica.

Las políticas expresadas en este plan son de obligatorio cumplimiento para todo el personal de la NUEVA LICORERA DE BOYACÁ.

3. MARCO LEGAL.

NORMA	DESCRIPCION
Ley estatutaria 1266 del 31 de diciembre de 2008	Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1273 del 5 de enero de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley estatutaria 1581 de 2012	Ley de protección de datos personales, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional
Decreto 1377 de 2013	Por el cual se reglamenta la Ley estatutaria 1581 de 2012
NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos
NTC/ISO 27002:2013	Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

4. PLAN DE SEGURIDAD INFORMATICA

Esta primera fase consiste en identificar y saber qué se tiene en la NUEVA LICORERA DE BOYACA, es decir, **hacer un inventario de los bienes** de la Nueva Licorera de Boyacá; para determinar el valor de lo que se quiere proteger.

Este conjunto de bienes incluirá sistemas informáticos, software, hardware, equipo humano, equipo técnico y demás herramientas que posibilitan el funcionamiento.

4.1. CARACTERIZACIÓN DEL SISTEMA INFORMATICO

El sistema informático de la NUEVA LICORERA DE BOYACA está soportado en los medios informáticos que se describen en el Anexo No. 1 (Inventario tecnológico, procedimiento: activos de información), que incluye un servidor, computadoras de mesa y portátiles, y una red local (tendido y elementos activos) que brinda servicio para la comunicación de información pertinente a las áreas de:

- GERENCIA,
- SUBGERENCIA ADMINISTRATIVA Y FINANCIERA,
- SUBGERENCIA TECNICA Y DE PRODUCIÓN Y
- SUBGERENCIA DE MERCADEO.

- El servidor tiene la función: alojamiento de Aplicaciones, base de datos, y transferencia de ficheros.

- Las aplicaciones y bases de datos en explotación son
    - Sistema Pradma: base de datos de software contable con motor SQL SERVER

- El cableado de la red está soportado por cable UTP categoría 5e, 10-100 Mb, con topología estrella (Anexo No 2. MAPA DE ESTRUCTURA DE RED), protegido físicamente por canaletas.

- Las estaciones de trabajo cuentan con:

    - Sistemas operativos:
        - Windows 10 home basic licencia individual
        - Windows 7 pro licencia individual,

    - Suite de oficina: Microsoft office 2016 licenciamiento por molp

    - Antivirus: Avast licenciado individualmente, por el término de dos años

    - Servicio de internet: Fibra óptica de 400 Mb, conectada en el rack principal a un modem propiedad de la empresa proveedora del servicio y conectada al Reuter principal.

    - Proveedor de internet: COLOMBIA MAS TV;

    - Dominio: nlb.com.co, permite el intercambio de información interna y externa, básicamente a través de las cuentas de correo electrónico empresarial.

4.2. RESULTADO DEL ANALISIS DE RIESGO

Ver documento: procedimiento para abordar riesgos del sig pe-de-sig-pr-04 y 4.1. Anexo 1. Definiciones administración de riesgo.

4.2.1. Determinación de las necesidades de protección mediante la evaluación de los riesgos.

- Los bienes informáticos más importantes para la gestión de la entidad y por lo tanto, que requieren de atención especial desde el punto de vista de la

protección, de acuerdo con el inventario y considerados de importancia crítica por el peso que tienen dentro del sistema.

- La red LAN de trabajo
- El servidor de aplicaciones y almacenamiento.
- Las bases de datos del sistema PRADMA con sus módulos
- El servicio de correo electrónico

- Amenazas de mayor impacto sobre la entidad en caso de materializarse sobre los bienes a proteger.

  - El acceso no autorizado a la red, tanto producto de un ataque externo como interno.
  - Pérdida de disponibilidad (caída del servicio de internet, red LAN, falla del servidor).
  - La sustracción, alteración o pérdida de datos (intencional o accidental).
  - Fuga de información clasificada (espionaje industrial)
  - La introducción de programas malignos.
  - El empleo inadecuado de las tecnologías y sus servicios.
  - Catástrofes Naturales.

- Áreas de mayor peso de riesgo y sus amenazas.

  - Vulnerabilidad de contraseñas de los usuarios, irresponsabilidad en su manejo y deficiente control de acceso de visitantes y funcionarios.
  - El área de los servidores de la red (acceso no autorizado y pérdida de disponibilidad).
  - Área de producción (alteración o pérdida de datos digitales o físicos, fuga de información clasificada, pérdida de disponibilidad y la introducción de programas malignos, o cualquier anomalía en la línea de producción)
  - La dependencia administrativa y financiera (alteración o pérdida de datos y documentos, pérdida de disponibilidad y la introducción de programas malignos)
  - La oficina Gerencia, (fuga de información clasificada)
  - La oficina de mercadeo (fuga de información clasificada y reservada, alteración o pérdida de datos y documentos, pérdida de disponibilidad y la introducción de programas malignos)
  - La oficina Planeación (fuga de información clasificada y reservada)
  - La oficina Control Interno (fuga de información clasificada y reservada)
  - Zona de almacenamiento (alteración o pérdida de datos y documentos, pérdida de disponibilidad y la introducción de programas malignos)

4.3. Políticas de Seguridad Informática

(Ver documento: cartilla de política de la Nueva Licorera de Boyacá)

4.4. Medidas y procedimientos

4.4.1. Clasificación y control de los bienes informáticos.

Medidas:

- Los bienes informáticos deberán estar identificados y controlados, hasta nivel de componentes.
- Cada uno de los bienes informáticos debe estar puesto bajo la custodia documentada legalmente de una persona que, actuando por delegación de las subgerencias, es responsable de su protección.
- Se realizarán auditorías periódicas para comprobar el control de Tecnologías Informáticas.
- Cada ordenador contara con un registro en el software de hojas de vida de cada uno de los equipos donde se registrarán todos los cambios que ocurran con el equipo.
- La subgerencia administrativa y financiera junto con almacén son los responsables del control de los medios informáticos a través de los diferentes procesos de sistema integrado gestión.

Número del Procedimiento	Procedimiento	Actividades a desarrollar	Responsable
Procedimiento No 1	Alta de Medios Informáticos para su uso.	1. Realizar controles sobre los bienes informáticos que se encuentran en cada departamento según el inventario.	Almacén
		2. Elaborar informe con los resultados de cada control y ponerlo en conocimiento de la subgerencia administrativa y financiera.	Almacén
		3. Notificar al profesional en sistemas la incorporación de cualquier medio informático a la Nueva Licorera de Boyacá.	Almacén.
		4. Garantizar que la oficina donde se ubique el medio informático cuente con las medidas de protección física requeridas.	Profesional en sistema.
		5. Instalar el software autorizado a utilizar en el área a la que fue asignado el medio informático, dejando constancia en el Registro de software autorizado.	profesional de sistemas.
		6. Integrar el equipo a la red de la Entidad y dejar en funcionamiento el equipo.	
		7. Firma del Acta de Responsabilidad Material que incluye el Expediente Técnico del medio informático.	Funcionario.
		8. Capacitar al personal encargado de la operación y protección del medio informático en materia de Seguridad Informática. .	Profesional en sistema

Procedimiento No. 2	Control de Medios Informáticos	1. Aplicar a cada PC la herramienta de software Everest para obtener los datos de sus componentes. 2. Confeccionar las hojas de vida de los equipos tecnológicas informáticos. 3. Velar porque las hojas de vida de los equipos tecnológicos informáticos se encuentren actualizados y se registren en ellos todos los cambios.	Profesional en Sistemas. Profesional en sistemas Profesional en sistemas
Procedimiento No. 3:	Asignación y control de Medios Informáticos Portátiles.	1. Solicitar por escrito a la subgerencia administrativa y financiera la asignación del Medio Informático Portátil 2. Una vez aprobada la solicitud, se notifica al profesional de sistemas para que proceda recoger el medio del almacén o de quien lo tenga en custodia. 3. Prepara el medio informático con el software autorizado necesario para su uso. 4. Entrega el medio informático al funcionario que hará uso del mismo, dejando constancia ******* 5. Solicita autorización escrita a la subgerencia administrativa y financiera, para la entrada y salida de la Entidad del bien informático. 6. Evalúa y autoriza el uso del bien informático fuera de las instalaciones de la Entidad. 7. Garantiza en el acceso principal de la Entidad que la salida y entrada de computadoras portátiles se realice por el personal autorizado.	Funcionario. Almacén y Profesional en sistemas Profesional en sistemas. Profesional en sistemas Funcionario Subgerencia administrativa y financiera Profesional de sistemas

4.4.2. Del personal

Las medidas y procedimientos de este acápite tienen como objetivo garantizar el cumplimiento de las funciones y responsabilidades de las personas vinculadas con las tecnologías y sus servicios, así como la documentación de las mismas.

Medidas:

- En el proceso de selección del personal que se incorpora a Nueva licorera de Boyacá, en caso que su trabajo se vincule con las tecnologías informáticas, se incluirá una valoración de su nivel de preparación.
- La subgerencia administrativa y financiera y talento Humano será la responsable de la valoración de la preparación de cada trabajador, la que requerirá las subgerencias. Debe quedar documentado el resultado de esta evaluación, así como el plan de capacitación en caso que se requiera.

- La subgerencia administrativa y financiera y talento Humano garantiza que en el expediente laboral de cada trabajador que se vincula con las tecnologías informáticas se incluya:
- Obligación de la entidad en cuanto a la preparación del personal

Número del Procedimiento	Procedimiento	Actividades a desarrollar	Responsable
Procedimiento No. 4	Selección, preparación y responsabilidad del personal respecto a la Seguridad Informática	La subgerencia administrativa y financiera – talento humano autoricen al profesional de sistemas, Se Dara a conocer las diferentes políticas de seguridad en la información con el fin de verificar el que hacer, como hacerlo	Subgerencia administrativa y financiera-Profesional en sistemas
Procedimiento No. 5	Otorgar/Retirar acceso de personas a las Tecnologías de Información (conexión a la red, correo e Internet).	Se realiza la creación de perfil de usuario con los permisos correspondientes a su actividad	Subgerencia administrativa y financiera /profesional en sistemas
Procedimiento No. 6	Otorgar acceso de personas externas al Nueva Licorera de Boyacá a las Tecnologías de Información	Los visitantes se pueden conectar a la red wifi de la Nueva Licorera de Boyacá a través del usuario INV_NLB. Este usuario está restringido solo a navegación	Subgerencia administrativa y financiera/profesional en sistemas
Procedimiento No. 7	Otorgar/Retirar acceso de usuarios al sistema contable PRADMA	Los nuevos usuarios / retiros del software Contable PRADMA serán configurados con la autorización de la subgerencia administrativa y financiera por el profesional administrador del software	Subgerencia administrativa y financiera/profesional administrador del software PRADMA
Procedimiento No. 8	Otorgar/Retirar acceso de usuarios a otras Aplicaciones y Servicios instalados.	Los nuevos usuarios/retiros de otras aplicaciones serán configurados con la autorización de subgerencia administrativa y financiera por el profesional administrador de dichas aplicaciones	Subgerencia administrativa y financiera/profesional administrador de aplicaciones

4.4.3. Seguridad Física y Ambiental.

- El equipo que cause baja o sea destinado para otras funciones será objeto de revisión por parte del profesional en sistemas, para evitar que la información que contiene pueda usarse y ser comprometida.
- Los dispositivos de almacenamiento que contengan información clasificada se destruirán físicamente, autorizado por la subgerencia administrativa y financiera.
- Para lograr la baja de los bienes informáticos se creará una comisión integrada por la subgerencia administrativa quien la preside, planeación, control interno y el profesional de sistemas.

Medidas generales para todas las áreas con tecnologías informáticas:

- Todos los tomacorrientes tendrán señalizado el tipo de voltaje que suministran para evitar accidentes o incendios.
- Los usuarios antes de conectar o desconectar los equipos de la red eléctrica chequearán que estos estén apagados.
- Contar con fuentes de respaldo de energía y estabilizadores de voltaje para cada computadora.
- En el caso de las áreas donde se procesan informaciones clasificadas o limitadas se tendrá en cuenta la posición del equipamiento, garantizando que

las computadoras estén situadas de forma tal que se impida ver el monitor por personas que entren al área.

Medidas para el ahorro de energía en todas las estaciones de trabajo.

- Activar el Modo de bajo consumo o de <espera> configurando la opción de ahorro para el monitor, disco duro y la inactividad del PC. Se recomienda entre cinco y diez minutos para el monitor y para el disco duro entre 5 y 30 minutos para la opción inactividad del PC.
- Habilitar el modo de hibernación. Se recomienda seleccionar como rango de tiempo para pasar al modo de hibernación un tiempo no menor de dos horas y no mayor de 6 horas.
- Desconectar los equipos después del horario laboral.

Medidas para el mantenimiento y reparación de las tecnologías informáticas.

- Las reparaciones menores y los mantenimientos se realizan por profesional de sistemas y las reparaciones mayores por entidades contratadas.
- Siempre que se realice el mantenimiento o la reparación de un equipo en la propia entidad se hará en presencia de una persona del área respectiva. Si el equipo contiene información clasificada y/o limitada debe estar presente el usuario del mismo.
- En caso de que sea necesario el traslado de un equipo fuera de la entidad, deberá reflejarse el movimiento del medio básico, además de actualizar los controles internos que indiquen el lugar donde se encontrará el equipo, su tiempo de permanencia en el taller y el técnico encargado de la reparación.
- Si se trata de una máquina contentiva de información clasificada y/o limitada, el profesional de sistemas, velará por que antes de extraer la computadora se retire el disco duro del equipo y si esto último no es posible, la información que contiene debe ser salvada y borrada físicamente del disco antes de su salida de la entidad. Especial atención se presta a los equipos que contengan información que permita recuperar contraseñas o datos que faciliten la comisión de alguna acción delictiva por parte de terceros.

Medidas para el Control de Acceso a oficinas:

Pueden ingresar a todas las oficinas:

- Miembros de salud y Seguridad en el trabajo para verificar el cumplimiento de las medidas de protección física.
- El profesional de sistemas para verificar el cumplimiento de las medidas de seguridad informática y la protección de la información.
- El personal de soporte técnico para el mantenimiento al sistema informático.
- Miembros del equipo que realiza las auditorías, en cumplimiento de esta tarea.
- Los máximos niveles de Dirección de la entidad.

Número del Procedimiento	Procedimiento	Actividades a desarrollar	Responsable
Procedimiento No. 9	Bajas de los bienes informáticos.	1. Definir el equipo informático al que se le dará baja.	Subgerencia administrativa y financiera/profesional en sistemas
		2. Recoger el equipo informático del área donde se encuentra y trasladarlo a la oficina del profesional en sistemas de Informática.	Profesional en sistemas
		3. Emitir diagnóstico y concepto técnico justificando por que se da de baja	Profesional en Sistemas
		4. Da baja al equipo informático de los Activos Fijos Tangibles (AFT).	Almacén/Profesional en Sistemas
		5. Desactivación del equipo, separando las partes reciclables.	Profesional en sistemas
Procedimiento No. 10	Bajas de los bienes informáticos que contengas Información Oficial Clasificada	1. Revisar el equipamiento propuesto para baja.	Profesional en sistemas
		2. Borrar la información de los bienes informáticos con información clasificada antes de entregarlos a informática con alguna herramienta de borrado seguro.	Profesional en sistemas
		3. Destruir físicamente los medios de almacenamiento que contengan información clasificada.	Profesional en sistemas
		4. Confeccionar el expediente de baja de la información clasificada almacenada en el bien informático.	Almacen/Profesional en sistemas
		5. Aplicar Procedimiento Bajas de bienes informáticos.	Almacen/profesional en sistemas
Procedimiento No. 11	Mantenimiento a Equipos	1. Según cronograma de mantenimiento preventivo y correctivo, 1 vez al año se le da mantenimientos a los Equipos.	Subgerencia administrativa y financiera/profesional en sistema
		2. Registra en el Expediente Técnico del equipo la fecha del mantenimiento y el nuevo sello asignado.	Profesional en sistemas
		3. Revisa que se deje constancia en los Expedientes Técnicos del mantenimiento realizado.	Profesional en sistemas
Procedimiento No. 12	Autorización y control sobre los movimientos de los bienes informáticos	1. Solicitar autorización por escrito a la Subgerencia administrativa y financiera para el movimiento de las tecnologías, fundamentando en que consiste el movimiento, los motivos y si es temporal el tiempo requerido.	Profesional en Sistemas
		2. Aceptada la solicitud se procede a realizar el movimiento de las tecnologías, especificando el tiempo de vigencia de la autorización e informar almacén.	Profesional en sistemas
		3. Revisar antes de su salida (entrada) de la entidad las tecnologías autorizadas a trasladar, precisando la existencia y estado de sus partes y componentes,	Profesional en sistemas

		si contienen información y de qué tipo, así como lo relacionado con el control antivirus. 4. Consignar el movimiento en el Registro de hoja de vida de equipos, especificando la fecha en que se produce, los datos del equipo objeto del movimiento, de qué lugar se extrae o proviene y a qué lugar se lleva y motivo por el que se realiza el movimiento. 5. Controlar el cumplimiento de las autorizaciones sobre el movimiento de las tecnologías y su registro adecuado.	Almacén/profesional en sistemas Profesional en sistemas

4.4.4. Seguridad de Operaciones:

La gestión del sistema de seguridad implica el control de las acciones que se realizan dentro del sistema informático y su garantía de que se ajustan a las políticas de seguridad establecidas para el empleo de las tecnologías y sus servicios. Para ello la Seguridad de Operaciones va dirigida a lograr la eficiente gestión de la seguridad y garantizar que se cumplan las regulaciones vigentes en el país.

- El profesional en sistemas designado realiza las tareas vinculadas con la administración de la red, los sistemas y los diferentes servicios.
- El cambio de contraseñas corresponde al profesional en sistemas.
- La introducción de nuevas tecnologías de la información en la Entidad debe estar incluida en el Plan Anual de adquisiciones, el cual es aprobado por el Comité Institucional de Gestión y desempeño.
- Las aplicaciones que se utilizan en la entidad son las aprobadas por el Comité Institucional de Gestión y desempeño

Número del Procedimiento	Procedimiento	Actividades a desarrollar	Responsable
Procedimiento No. 13	Corrección de errores y brechas de seguridad	1. Preservar las trazas de auditoría de los sistemas en los soportes habilitados al efecto por un tiempo no menor de un año. 2. Ejecutar las herramientas de seguridad autorizadas en la entidad. 3. Analizar los resultados que arrojaron las herramientas y su correspondencia con el nivel de seguridad previsto en la entidad. 4. En caso de detectarse nuevas vulnerabilidades, proponer las acciones necesarias para su evaluación y determinación de las modificaciones requeridas para su eliminación. 5. Informar al profesional en sistemas, las acciones de emergencias ejecutadas para garantizar la seguridad del sistema. 6. Documentar en el Registro de Incidencias de Seguridad Informática las acciones ejecutadas.	Profesional en sistemas

		7. Notificar a la Dirección Nacional de Seguridad y Protección (Ver Anexo 7.2.16) y a la OSRI (Ver Anexo 7.2.19) del incidente. 8. Determinar si es necesario realizar cambios en el sistema de seguridad informática diseñado. Diseñar la nueva estrategia a seguir. 9. Realizar un control trimestral de este procedimiento e informar de sus resultados a la Subgerencia administrativa y financiera	
Procedimiento No. 14	Realización de inspecciones de Seguridad Informática.	1. Confeccionar el Plan de Inspecciones de Seguridad Informática de la Entidad. 2. Presentar el plan de inspecciones a la subgerencia administrativa y financiera para su aprobación. 3. Ejecutar el plan de inspecciones según la fecha planificada. 4. Chequeará las tareas funcionales que debe efectuar cada cual de acuerdo a su responsabilidad y a las políticas de seguridad informática. 5. Realizará inspecciones independientes a cada una de las máquinas, efectuando pruebas en las que trate de violentar las medidas de seguridad. 6. Se anotará los resultados en el Registro de Inspecciones 7. Aquellos hechos que comprometan la seguridad informática serán anotados en el Registro de incidencias (Ver Anexo 7.2.18). 8. Notificar a la Dirección Nacional de Seguridad y Protección (Ver Anexo 7.2.16) y a la OSRI (Ver Anexo 7.2.19) del incidente. 9. Confeccionar un informe con los resultados de la inspección y enviarlo al director de la Administración Interna.	Profesional en sistemas
Procedimiento No. 15	Introducción de nuevos sistemas informáticos, actualizaciones y nuevas versiones	1. El profesional de sistemas solicita a la subgerencia administrativa y financiera, la aprobación para la instalación o actualización de nuevas de aplicaciones. 2. Aprobar o denegar solicitud. 3. Comprueba que el nuevo software o aplicación cumple con el sistema de seguridad establecido en la institución. 4. Instala y configura el nuevo sistema informático, actualización o versión.	Profesional en sistemas Subgerencia administrativa y financiera Profesional en sistemas Profesional en sistemas

4.4.5. Identificación, Autenticación y Control de Acceso.

Las medidas y procedimientos de este acápite tienen como objetivo gestionar el acceso a la información de forma segura, garantizando el acceso de usuarios autorizados e impidiendo el acceso no autorizado a los sistemas de información.

- Se establecerán identificadores de usuarios en las PCs, sistemas y servicios informáticos en la red.

- Los identificadores de usuarios se darán por el profesional en sistemas, con permisos de configuración red, al causar alta de un usuario al trabajo con las tecnologías de la información, lo cual será notificado por la subgerencia administrativa y financiera
- Estos identificadores serán eliminados por el profesional de sistemas tan pronto el trabajador cause baja.

Número del Procedimiento	Procedimiento	Actividades a desarrollar	Responsable
Procedimiento No.16	Control de la Identificación de usuario	1. Una vez que los usuarios estén creados como fue descrito en el procedimiento Otorgar/Retirar acceso de personas a las Tecnologías de Información, se revisará que los identificadores que se están utilizando correspondan con la situación de los trabajadores autorizados a trabajar con las tecnologías informáticas.	Profesional en sistemas
Procedimiento No. 17	Autentificación de usuario	1. Las Pc contarán con contraseñas que bloqueen el acceso al Setup. 2. La cuenta de administrador estará deshabilitada. 3. El trabajador accederá al ordenador con el usuario que le sea asignado por el profesional en sistemas o el administrador del software PRADMA 2. Realizar periódicamente un Control de la Autenticación de usuarios.	Profesional en sistemas Profesional en sistemas Profesional en sistemas Profesional en sistemas
Procedimiento No. 18	Autentificación de usuario en ordenadores desconectados de la red	1. Las Pc contarán con contraseñas de Inicio del SO, Setup, cuentas de administrador y usuario estándar. 2. Cada usuario poseerá una contraseña para acceder a la PC en una sesión independiente. 3. Habilitar el uso de protectores de pantalla con contraseña, lo que evitará que la información sea vista en momentos de inactividad y la entrada de intrusos. 4. Los usuarios se autenticarán para hacer uso de su cuenta de usuario en la red local y los servicios autorizados. 5. Realizar periódicamente un Control de la Autenticación de usuarios.	Funcionarios/profesional en sistemas Funcionario/profesional en sistemas Funcionarios Funcionarios/profesional en sistemas Profesional en sistemas

Procedimiento No. 19	Cambio de contraseña de los servicios de correo e Internet.	1. Solicitar al Administrador de red o de correos empresariales (profesional en sistema) el cambio de contraseñas de los servicios de correo 2. Cambiar la contraseña de la cuenta, respetando las políticas definidas para las contraseñas. 3. Chequear que en los servicios de correo e Internet estén implementadas las políticas de contraseñas definidas.	Funcionarios Funcionario/profesional en sistemas Profesional en sitemas
Procedimiento No. 20	Cambio de contraseña de usuario del dominio.	1. Cada 3 meses la contraseña de usuario del dominio expira, por lo que al cumplirse el plazo se notificara al iniciar la sesión que debe realizarse el cambio de la misma. 2. Cambiar la contraseña antes del plazo de 3 meses a través de la combinación de teclas Ctrl+Alt+Supr.	Profesional en sistemas Profesional en sistemas/funcionario

4.4.6. Seguridad ante programas malignos.

En las estaciones de trabajo y servidores se cuenta con el Antivirus Avast Business Antivirus. Este producto se mantendrá debidamente actualizado. Para ello el profesional en sistema realizara control periódicamente.

- Cada funcionario responsable de efectuar el chequeo de todos los soportes (Discos externos, Memoria Usb, CD, DVD) de propiedad personal o de otra entidad que se autoricen introducir en el ordenador antes de su utilización.
- El profesional en sistemas será la encargada de efectuar la descontaminación de los ordenadores ante la aparición de programas malignos.
- El Profesional de sistemas es el encargado de la correcta actualización del Software Antivirus en el Servidor.
- La actualización del Software Antivirus de las máquinas y Servidores se realizará diariamente, de forma programada.
- La actualización del Software Antivirus en los ordenadores donde se procesa Información Oficial Clasificada es responsabilidad del profesional en sistemas.
- Cada funcionario es responsable de comprobar la correcta actualización del Software Antivirus instalado en el ordenador a su cargo.

Número del Procedimiento	Procedimiento	Actividades a desarrollar	Responsable
Procedimiento No. 21	Actualización del Software Antivirus en el Servidor	1. Semanalmente se descarga a las 6:00 am de forma automática desde la url: www.business.avast.com la actualización del Antivirus	Profesional en sistemas

		2. Chequear si la actualización se descargó con efectividad. 3. Chequear periódicamente la actualización del Antivirus en el Servidor.	Profesional en sistemas Profesional en sistemas

4.4.7. Respaldo de la información

Las medidas y procedimientos de respaldo que se implementen garantizaran mantener la integridad y disponibilidad de la información y de las instalaciones de procesamiento de la información frente a cualquier eventualidad.

- Se realizarán copias de seguridad de la información y del software que se determine y se comprobarán con regularidad.
- Cada trabajador será responsable de la información que guarde en los accesos públicos de la red y de la periodicidad con que realice las salvas personales.
- La subgerencia administrativa y financiera / profesional en sistemas son los responsables de organizar la salva de la información de las áreas respectivas, definiendo la información a salvar
- En el caso de la información clasificada y/o limitada la salva debe ser hecha sólo por personal autorizado para el procesamiento de este tipo de información.
- Cada área dispondrá de un disco externo para la salvaguarda de la información clasificada y/o limitada.

Número del Procedimiento	Procedimiento	Actividades a desarrollar	Responsable
Procedimiento No.22	Actualización del Software Antivirus en el Servidor	1. Semanalmente se descarga a las 6:00 am de forma automática desde la url: www.business.avast.com la actualización del Antivirus 2. Chequear si la actualización se descargó con efectividad. 3. Chequear periódicamente la actualización del Antivirus en el Servidor.	Profesional en sistemas Profesional en sistemas Profesional en sistemas
Procedimiento No. 23	Respaldo de la Información del Servidor de la Red local NLB Nivel central.	1. Semanalmente, según el procedimiento de copias de seguridad del SIG de la NLB, se efectúa el respaldo de la información de cada Servidor. 2. La copia es alojada de manera temporal en el Servidor de aplicaciones y/o de base de datos correspondiente y luego se almacena en un disco externo de 2 TB. 3. Dejar constancia en el Registro en la bitácora de copias de seguridad sobre el éxito o la falla de la salva en el campo Observaciones. 4. Controlar periódicamente el cumplimiento de este procedimiento.	Subgerencia administrativa y financiera/profesional en sistemas profesional en sistemas profesional en sistemas profesional en sistemas
Procedimiento No. 24	Respaldo de la Información Oficial Clasificada.	1. Solicitar el disco externo correspondiente de la información oficial clasificada donde se almacenará la Copia.	Profesional en sistemas

		2. Crear una carpeta con la fecha en que se realiza la copia en el disco externo.	Profesional en sistemas
		3. Almacenar en la carpeta la Información Oficial Clasificada alojada en el servidor (base de datos PRADMA, contabilidad).	Profesional en sistemas
		4. Entregar el disco externo con la información oficial clasificada a subgerencia administrativa y financiera para su custodia.	Profesional en sistemas
		5. Controlar periódicamente el cumplimiento de este procedimiento.	Profesional en sistemas
Procedimiento No. 25	Respaldo de Aplicaciones	1. Solicitar el disco externo de la información oficial clasificada correspondiente donde se almacenará la copia de los datos de las aplicaciones.	Profesional en sistemas
		2. Realizar copias seguras y completas de la información con periodicidad semanal o máximo quincenal.	Profesional en sistemas
		3. Probar regularmente los soportes de respaldo para verificar que las copias efectuadas son eficaces.	Profesional en sistemas
		4. Comprobar regularmente los procedimientos de restauración de copia de seguridad.	Profesional en sistemas
		5. Dejar constancia en el formato bitácora de copias de seguridad, sobre el éxito o la falla de la copia en el campo Observaciones.	Profesional en sistemas
		6. Controlar periódicamente el cumplimiento de este procedimiento.	Profesional en sistemas

4.4.8 Seguridad en Redes

- El profesional en sistemas regularmente deberá chequear el tráfico de la red para detectar variaciones que pueden ser síntoma de mal uso de la misma.
- El profesional en sistemas es quien monitorea las conexiones activas y los puertos en la red para saber qué puertos están habilitados y chequear la seguridad de los mismos.
- No administrar remotamente la red mediante conexiones conmutadas a través de las redes públicas de transmisión de datos.
- El profesional de sistemas será el encargado de auditar los directorios para poder determinar los ataques que se realizan sobre ellos.
- El profesional de sistemas deberá actualizar el sistema periódicamente con los últimos Service Pack y parches de seguridad para resguardar el sistema de las últimas vulnerabilidades conocidas.
- El profesional en sistemas deberá establecer los permisos de acceso adecuados (administrador, system y usuarios autenticados).

Número del Procedimiento	Procedimiento	Actividades a desarrollar	Responsable
Procedimiento No.26	Auditoria de eventos	1. Revisar diariamente los registros de los eventos generados. 2. Ante cualquier anomalía que se detecte, investigar las causas y determinar si se está ante algún incidente de seguridad. 3. Mantener la disponibilidad y la actualización de las herramientas que garantizan la auditoria de los eventos. 4. Controlar periódicamente el cumplimiento de este procedimiento. Responsable: Especialista de Seguridad Informática.	Profesional en sistemas
Procedimiento No. 27	Revisión de las trazas de navegación	1. Se visualizan los logs mediante el Internet Access Monitor. 2. Se analiza la actividad de los usuarios (Sitios visitados, fechas y horarios de las consultas, información descargada, etc.) 3. Si se detecta alguna violación se realiza un informe detallado mostrando evidencia de la violación. 4. Se notifica por escrito la violación al subgerencia administrativa y financiera. 5. Se envía reporte de la violación a la Dirección Nacional de Seguridad y Protección.	Profesional en sistemas Profesional en sistemas Profesional en sistemas Profesional en sistemas Profesional en sistemas
Procedimiento No. 28	Aplicación de mecanismos que implementan las políticas de Seguridad aprobadas.	1. Al incorporarse un nuevo ordenador al Sistema informático del NLB, se incorpora a la red local. 2. Una vez en el dominio, el equipo acatara todas las políticas aprobadas que fueron definidas en Políticas de Seguridad Informática. 3. Chequear periódicamente que los ordenadores cumplan con las políticas establecidas.	Profesional en sistemas
Procedimiento No. 29	Acciones de respuesta en caso de ocurrencia de incidentes o actividades nocivas. Gestión de Incidentes de Seguridad	1. Informar al profesional de sistemas la incidencia o actividad nociva. 2. Verificar la ocurrencia del incidente y aislar el equipo de la red 3. En caso de implicaciones de seguridad de la NLB, denunciar ante la autoridad competente 4. Combatir el origen de la actividad nociva	Funcionario Profesional en Sistemas Funcionario / Profesional en sistemas Profesional en sistemas

4.4.9. Gestión de Incidentes de Seguridad.

Número del Procedimiento	Procedimiento	Actividades a desarrollar	Responsable
Procedimiento No.30	Recepción y valoración del incidente	1. Informar inmediatamente sobre el incidente de seguridad y diligenciar el formato correspondiente. 2. Escuchar atentamente al funcionario sobre los eventos que provocaron el incidente (determinar la	Funcionario Profesional de sistemas

		intencionalidad o accidentalidad de los procedimientos previos al incidente)	
		3. Determinar la trascendencia del incidente de seguridad, de acuerdo con la información afectada y se trasladará al nivel directivo	Profesional de sistemas
		4. Determinar el tipo de incidencia disciplinaria generada	Nivel directivo – control interno
Procedimiento No. 31	Tramite del incidente	1. Verificar en la bitácora de gestión del conocimiento si existen antecedentes del incidente.	Profesional en sistemas
		2. Determinación de la información afectada o presumiblemente afectada e informar a la alta dirección	Profesional en sistemas
		3. Determinación de las consecuencias de la vulneración de seguridad de la información y sus posibles implicaciones a nivel empresarial	Control interno, - Alta dirección
		4. Determinación de acciones correctivas (internas) y ante las instancias correspondientes (externas) según los directivos a cargo de la investigación.	Control interno, - Alta dirección
		5. Sancionar según determinación del impacto de la falta y comunicar a talento humano	Nivel Directivo - Talento Humano
Procedimiento No. 31	Solución incidente	1. Recopilación de determinaciones del nivel directivo y control interno respecto del impacto de la incidencia y tomar los correctivos solicitados por la alta dirección en cuanto a la información afectada.	Profesional de sistemas
Procedimiento No. 32	Gestión del conocimiento	1. Abrir registro (archivo o carpeta) del incidente	Profesional de Sistemas
		2. Descripción técnica de las fallas de seguridad que originaron la vulneración de seguridad	Profesional en Sistemas
		3. Registro detallado de las medidas correctivas ordenadas por el nivel directivo.	Profesional de sistemas.

4.5. ANEXO PLAN SEGURIDAD DE LA INFORMACIÓN:

ANEXO 1. INVENTARIO TECNOLÓGICO (Ver documento Inventario tecnológico)

ANEXO 2. ESTRUCTURA DE LAN NUEVA LICORERA DE BAOYACA.