La que más billete da

MANUAL DE POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD DE LA INFORMACIÓN

LOTERÍA DE BOGOTÁ

2023

Contenido

SIGLAS Y ABREVIATURAS

AltaTIC: Alta Consejería Distrital de TIC.

MINTIC: Ministerio de Tecnologías de la Información y las Comunicaciones.

MSPI: Modelo de Seguridad y Privacidad de la Información

TIC: Tecnologías de la Información y las Comunicaciones.

VPN: Virtual Private Network - Red Privada Virtual.

WIFI: Wireless Fidelity - Fidelidad inalámbrica.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Establecer las políticas de seguridad de la información que deben ser aplicadas por los funcionarios, contratistas, entes de control, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y de la LOTERÍA DE BOGOTÁ, compartan, utilicen, recolecten, procesen, intercambien o consulten su información.

1.2. OBJETIVOS ESPECÍFICOS

1. Establecer un esquema de seguridad de la información clara, transparente y aplicable bajo la responsabilidad de la LOTERÍA DE BOGOTÁ en cuanto a la administración del riesgo se refiere.

2. Proteger el talento humano, la información y los recursos tecnológicos utilizados por la LOTERÍA DE BOGOTÁ frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información de la entidad.

3. Formular lineamentos en seguridad de la información para la LOTERÍA DE BOGOTÁ que permitan proteger los activos de información, de tal manera que se preserve su confidencialidad, integridad y disponibilidad de acuerdo con el nivel de criticidad establecido en la clasificación y valoración de dichos activos realizada en la entidad.

4. Definir directrices para el correcto uso de los componentes de hardware, software, información física e información digital de la LOTERÍA DE BOGOTÁ, con el fin de contribuir a la mitigación del riesgo de ocurrencia de incidentes de seguridad de la información.

2. ALCANCE

Este documento describe las políticas de seguridad de la información definidas por la LOTERÍA DE BOGOTÁ, teniendo en cuenta la política de Gobierno Digital establecida mediante el Decreto 1008 de 2018, el Modelo de Seguridad y Privacidad de la Información, la ley 1581 de 2012 de protección de datos personales y demás legislación aplicable.

Estas políticas se aplican en todo el ámbito de la LOTERÍA DE BOGOTÁ, que incluye los funcionarios, contratistas, entes de control, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la LOTERÍA DE BOGOTÁ, compartan, utilicen, recolecten, procesen, intercambien o consulten su información.

3. NORMATIVA

- Ley 527 de 1999. Ley de Comercio Electrónico y Firmas Digitales.
- Ley 594 de 2000. Ley General de Archivos.
- Ley 1712 de 2014, Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional
- Directiva 005 de 2005 de la Alcaldía mayor de Bogotá, “Por medio de la cual se

adoptan las Políticas Generales de Tecnología de Información y Comunicaciones aplicables al Distrito Capital".

- Circular 37 de 2018 Incidentes de ciberseguridad y modelo de seguridad y privacidad de la información MPSI del MINTIC

- Acuerdo 279 de 2007 Consejo de Bogotá. Lineamientos para la Política de Promoción y Uso del Software libre en el Sector Central, el Sector Descentralizado y el Sector de las Localidades del Distrito Capital.

- Ley 1581 de 2012 del Congreso de la República, "Por la cual se dictan disposiciones generales para la protección de datos personales".

- Decreto 1008 de 2018 del Ministerio de Tecnologías de la Información y las Comunicaciones, "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".

- Decreto 296 de 2008. Comité de Gobierno en Línea a la Comisión Distrital de Sistemas.

- Modelo Integrado de Planeación y Gestión – MIPG versión 4, marzo de 2021.

- Resolución 0500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones, "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".

- Modelo de Seguridad y Privacidad de la Información (MSPI), Política de Gobierno Digital, Ministerio de Tecnologías de la Información y las Comunicaciones – versión

4. 2021.

- CONPES 3995 de 2020 - Política Nacional de Confianza y Seguridad Digital.

- Circular No. 058 de 2009 de la Procuraduría General de la Nación Cumplimiento Decreto 1151 de 2008.

- Ley 1273 de 2009. Ley de Delitos Informáticos.

- Decreto 2364 de 2012. Firma electrónica.

- Decreto 2609 de 2012. Gestión documental (Compilado en el 1080 de 2015, Capítulo III).

- Circular 005 de 2012 emitida por el Archivo General de la Nación. Recomendaciones para llevar a cabo procesos de digitalización y comunicaciones oficiales electrónicas en el marco de la iniciativa “cero papel”.

- Decreto 1078 de 2015. Decreto Único Sectorial - Lineamientos generales de la Estrategia de Gobierno en Línea.

- Acuerdo 003 de 2015, Gestión de documentos electrónicos como resultado del uso de medios electrónicos. Archivo General de la Nación.

- Resolución 3564 de 2015 Reglamentaciones asociadas a la Ley de Transparencia y Acceso a la Información Pública. Ministerio de Tecnologías de la Información y las Comunicaciones.

- Circular No. 007 de 2015, Secretaría General de la Alcaldía Mayor de Bogotá. Lineamientos generales para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información.

- Conpes 3854 de 2016, Ministerio de Tecnologías de la Información y las Comunicaciones. Política Nacional de Seguridad Digital.

- Resolución 004 de 2017 Comisión distrital de Sistemas “Por la cual se modifica la Resolución 305 de 2008 de la CDS”

- Ley 1952 de 2019. Código General Disciplinario.

- Ley 1955 de 2019 Por el cual se expide el Plan Nacional de Desarrollo 2018- 2022 "Pacto por Colombia, Pacto por la Equidad"; Art. 147.

- Ley 1978 de 2019 Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones (TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.

4. GLOSARIO

Ver anexo 1.

5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

5.1. REVISIÓN DE LA POLÍTICA Y EL MANUAL DE POLÍTICAS

La política de seguridad de la información y el manual de políticas de seguridad de lainformación deben ser revisados y actualizados (en caso de ser necesario) al menos una vez al año o cuando haya cambios relevantes en el contexto estratégico de la LOTERÍA DEBOGOTÁ, con el fin de asegurar que sigan siendo adecuados a la estrategia y necesidadesde la organización. Esta actividad es responsabilidad del Comité Institucional de Gestión y Desempeño.

5.2. ORGANIZACIÓN DE LA SEGURIDAD

5.2.1. Roles y responsabilidades

Todo aquel que tenga acceso a la información de la LOTERÍA DE BOGOTÁ, será responsable de velar por la seguridad de la información a la que tiene acceso y de cumplir las políticas descritas en este documento; entre ellos están: funcionarios, contratistas, entes de control, proveedores y visitantes.

El incumplimiento de procedimientos o políticas de seguridad de la información por no atención de los comunicados oficiales no exime al funcionario, contratista, proveedor o visitante de las medidas que pueda tomar la LOTERÍA DE BOGOTÁ, como se menciona en la sección 6.4.3 de este documento.

El Oficial de Seguridad de la Información (OSI), asumirá la responsabilidad por el desarrollo e implementación de la seguridad de la información, comprobará el cumplimiento de las políticas, en caso de requerirse prestará asesoría a todo aquel que maneje información de la entidad, coordinará las actividades de la gestión de riesgos de la seguridad de la información con el apoyo de la oficina de planeación estratégica de la Lotería de Bogotá, para la identificación de controles y reportará al Comité Institucional de Gestión y Desempeño de la Lotería de Bogotá.

5.2.2. Separación de deberes

Todo aquel que tenga acceso a la información de la LOTERÍA DE BOGOTÁ, debe tener claramente definidas sus funciones u obligaciones, con el fin de reducir el uso no autorizado, indebido o accidental de los activos de información.

Todos los sistemas de información de la entidad, deben implementar reglas de acceso a los mismos, de tal forma que existan roles entre quien administre, opere,

mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

5.2.3. Contacto con autoridades y grupos de interés

La LOTERÍA DE BOGOTÁ mantendrá contacto con las autoridades competentes para el cumplimiento de la ley, organismos de control y autoridades de supervisión correspondientes. Adicionalmente, la Oficina de Gestión Tecnológica e Innovación cuenta con un directorio actualizado de autoridades y grupos de interés.

La Oficina de Gestión Tecnológica e Innovación mantendrá contacto con grupos especializados, foros y asociaciones profesionales en el campo de la seguridad de la información. Lo anterior, con el fin de estar al día con la información relacionada con la seguridad de la información, mejores prácticas y recibir advertencias de actualizaciones, ataques y vulnerabilidades del software y firmware utilizado en la LOTERÍA DE BOGOTÁ.

5.2.4. Seguridad de la información en la gestión de contratos

La seguridad de la información debe ser parte integral en la entidad y se debe asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de los contratos. Esto aplicará a cualquier contrato, independientemente de su naturaleza. Por lo tanto, es responsabilidad de los supervisores del contrato asegurar que se sigan las siguientes directrices:

Incluir cláusulas de seguridad de la información en el contrato.

Realizar valoración de los riesgos de seguridad de la información en la fase de estudios previos del contrato, para identificar los controles necesarios.

Hacer seguimiento a los riesgos y controles aplicados para tratar los riesgos, durante todas las fases del contrato.

5.3. DISPOSITIVOS MÓVILES Y TELETRABAJO O TRABAJO EN CASA

5.3.1. Dispositivos móviles

Se dispondrá de una red de invitados para la conexión de los equipos de visitantes a la Lotería, la cual permitirá la salida hacia Internet, pero no permitirá la conexión con equipos de cómputo o servidores de la LOTERÍA DE BOGOTÁ.

Las estaciones de trabajo y equipos portátiles que son propiedad de la LOTERÍA DE BOGOTÁ cuentan con software licenciado y protección contra código malicioso.

La LOTERÍA DE BOGOTÁ se reserva el derecho de monitorear y revisar los equipos de cómputo conectados a la red de la entidad.

La Lotería de BOGOTÁ debe suministrar el antivirus para todos los equipos de la entidad.

5.3.2. Teletrabajo o trabajo en casa

Cuando se requiera realizar labores de teletrabajo el jefe del área y/o dependencia a la cual pertenece el servidor o contratista, debe solicitar a la Oficina de Gestión Tecnológica e Innovación la configuración de una VPN petición a mesadeservicio@loteriadebogota.com, los servicios, ambientes y aplicativos a los cuales se requiere acceder. El servidor o contratista se debe comprometer a hacer

un uso adecuado de la VPN.

En los casos en los cuales el acceso y procesamiento de la información de la LOTERÍA DE BOGOTÁ, sea mediante la modalidad de teletrabajo, los responsables de estas actividades deben dar cumplimiento a las condiciones y restricciones definidas entorno a la seguridad de la información, tales como:

- Seguridad física.
- Acceso no autorizado a información o recursos.

5.4. SEGURIDAD DEL RECURSO HUMANO

5.4.1. Vinculación, desvinculación y cambio de cargo

En atención a los requisitos de la norma NTC-ISO/IEC 27001:2013 y la legislación aplicable con relación a la contratación pública, la vinculación laboral, retiro laboral y el cambio de cargo se llevarán a cabo siguiendo los procedimientos definidos para tal fin.

En la vinculación de los funcionarios o contratistas se deberá solicitar por talento humano, jefe de la oficina, líder de proceso o supervisor del contrato, la creación del usuario de red y de dominio; dicha solicitud deberá realizarse por petición al correo mesadeservicio@loteriadebogota.com.

5.4.2. Capacitación y entrenamiento en seguridad de la información

La LOTERÍA DE BOGOTÁ debe asegurar que todos los servidores, contratistas, proveedores, visitantes y todos aquellos con acceso a la información y que tengan definidas responsabilidades de seguridad de la información sean competentes (en

cuanto a capacitación formal y no formal) para desempeñar sus funciones u obligaciones.

La Oficina de Gestión Tecnológica e Innovación de la Lotería de Bogotá solicitará a la Unidad de Talento Humano incluya en el Plan Institucional de Capacitación (PIC) como mínimo una capacitación al año sobre temas de seguridad de la información, para lo cual la Oficina de Gestión Tecnológica e Innovación la gestionará y desarrolla. La solicitud de Talento Humano o supervisor del contrato enviado a mesadeservicio@loteriadebogota.com para la capacitación al servidor o contratista en los temas de seguridad., el cual hará parte del proceso de inducción de la LOTERÍA DE BOGOTÁ.

5.4.3. Procesos disciplinarios

Los procesos disciplinarios en la LOTERÍA DE BOGOTÁ se llevarán a cabo de acuerdo con la Ley 1952 de 2019 “Por el cual se expide el Código General Disciplinario”, por parte de la Oficina de Control Disciplinario Interno. A los procesos disciplinarios que adelanta con ocasión al incumplimiento de estas políticas, la LOTERÍA DE BOGOTÁ aplicará las normas de publicidad, reserva, seguridad de la información, entre otros.

5.4.4. Intercambio de información

Cuando se desee intercambiar información pública clasificada o publica reservada se deberá clasificar de acuerdo al caso:

- Para los organismos de control y autoridades de supervisión se generará una carta de Gerencia que implica la responsabilidad de la Lotería de Bogotá, para la entrega de la información y el compromiso del ente que recibe con

relación al manejo de dicha información en términos de seguridad y privacidad.

- Para los servidores y contratistas se encuentran en las cláusulas de confidencialidad de los contratos.
- Para terceros y partes interesadas se suscribirá un acuerdo de confidencialidad e intercambio de información y seguridad de la información entre las partes.

5.5. GESTIÓN DE ACTIVOS

5.5.1. Inventario de activos

Los líderes de las áreas responsables mantendrán actualizado el inventario de activos de la información de acuerdo.

5.5.2. Asignación de activos

La asignación de los activos de información se realizará en coordinación con Recursos Físicos y Sistemas, de acuerdo a la solicitud del jefe inmediato o supervisor del contrato realizada a través del correo mesadeservicio@loteriadebogota.com.

5.5.3. Uso aceptable de los activos

La información, archivos físicos, sistemas, servicios, y los equipos (ej. estaciones de trabajo, portátiles, impresoras, redes, internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos, entre otros), son activos de la entidad y se proporcionan a los servidores, contratistas y terceros autorizados, para cumplir con los propósitos de la Lotería de Bogotá.

Los servidores, contratistas, proveedores y visitantes de la entidad deben reportar los eventos de seguridad de la información identificados al correo mesadeservicio@loteriadebogota.com.

Se debe realizar aplicación del registro activo de la información con el que cuenta la Lotería de Bogotá, disponible en el link de transparencia https://www.loteriadebogota.com/wp-content/uploads/files/rfisicos/REGISTRO_ACTIVOS_INFORMACION.pdf , el cual reflejan la clasificación documental como la descripción del soporte.

Se deberá garantizar el diligenciamiento del Formato de Inventario Documental FR0 281 desde la producción de la información (Física y/o electrónica) independientemente su soporte, los cuales permiten el control seguimiento y cumplimiento durante del ciclo de vida de la información.

5.5.4. Devolución de activos

La devolución de activos se actualizará con la solicitud de almacén realizada al correo electrónico mesadeservicio@loteríadebogotá.com.

La devolución de equipos de cómputo o activos cuando se finalizan contratos o se presente retiro definitivo de la entidad o traslado de funciones, se hará por medio de la solicitud por parte de talento humano a través de correo electrónico mesadeservicio@loteríadebogotá.com.

5.5.5. Uso de equipos de cómputo

Está prohibido que personal ajeno a la Oficina de Gestión Tecnológica e Innovación,

destape o retire partes de los equipos de cómputo que pertenecen al inventario de la LOTERÍA DE BOGOTÁ.

La instalación de cualquier tipo de software o hardware en los equipos de cómputo es responsabilidad de la Oficina de Gestión Tecnológica e Innovación, por tanto, se debe realizar una solicitud al correo mesadeservicio@loteriadebogota.com para la realización de estas actividades.

Los equipos de cómputo no podrán ser trasladados del sitio asignado inicialmente, ni cambiar el funcionario o contratista al que le fue asignado, sin previo aviso la Oficina de Gestión Tecnológica e Innovación y Almacén.

Debe respetarse y no modificarse la configuración de hardware y software establecida por la Oficina de Gestión Tecnológica e Innovación.

Se restringe el acceso de medios extraíbles (USB, discos externos, CD, DVD, entre otros) para almacenamiento de información institucional en todas las estaciones de trabajo de la entidad, salvo las autorizadas explícitamente por la gerencia de la entidad.

Toda actividad informática (escaneos de seguridad, ataques de autenticación o de denegación de servicio, etc.) no autorizada que afecte tanto las redes corporativas como los sistemas de información de la LOTERÍA DE BOGOTÁ, está prohibida y dará lugar a los procesos disciplinarios y/o legales correspondientes establecidos en el punto 6.4.3 del presente manual.

Durante la permanencia en las instalaciones de la LOTERÍA DE BOGOTÁ, los equipos de cómputo externos deben estar conectados únicamente a la red de datos Wifi corporativa configurada por la Oficina de Gestión Tecnológica e Innovación, en

caso de requerir acceso a la red LAN o cableada, deben hacer la solicitud a través de la mesa de servicio, cualquier otro tipo de acceso no está autorizado y dará lugar a los procesos disciplinarios y/o legales correspondientes.

Los equipos de cómputo (CPU), servidores, teléfonos IP y equipos de comunicaciones, deben conectarse a los puntos de corriente eléctrica identificados como regulados (tapa naranja), el monitor debe conectarse a la toma de corriente normal (toma blanca).

La seguridad física e integridad de los equipos de cómputo que ingresen a las instalaciones de la LOTERÍA DE BOGOTÁ y que no son propiedad de la entidad, serán responsabilidad única y exclusiva de sus propietarios. La LOTERÍA DE BOGOTÁ, no será responsable por estos equipos en ningún caso.

5.5.6. Uso de internet

Está prohibido conectar cualquier dispositivo en modo Access Point para acceder a Internet, dentro de la red WAN de la entidad.

Queda prohibido a todos los funcionarios y contratistas acceder a cualquier página o dirección que contenga material pornográfico en cualquiera de sus variantes, o bien páginas que promuevan cualquier tipo de ideas que puedan ser consideradas ofensivas para las normas de la LOTERÍA DE BOGOTÁ tales como violencia, terrorismo, grupos al margen de la ley, discriminación, entre otras.

Se prohíbe el envío, descarga o visualización de información con contenido que atente contra la integridad moral personal, institucional o que conlleven a la comisión de algún delito.

Con el propósito de minimizar la probabilidad de saturación, interrupción, alteraciones no autorizadas y errores en la red de la LOTERÍA DE BOGOTÁ, no se permite el envío o descarga de información masiva como música, videos y/o software no autorizado.

Todo usuario es responsable del contenido de toda comunicación e información que se envíe o descargue desde su cuenta (correo, directorio activo y demás aplicaciones institucionales).

Todas las actividades realizadas en los sistemas de información de la LOTERÍA DE BOGOTÁ, podrán ser monitoreadas con el fin de preservar la seguridad informática de la entidad.

Los usuarios no deben intentar burlar o evadir los sistemas de seguridad y de control de acceso; acciones de esta naturaleza se consideran violatorias de las políticas de la entidad y de la ley y serán sancionadas de acuerdo con la Ley 1952 de 2019 “Por el cual se expide el Código General Disciplinario”.

5.5.7. Uso del correo institucional

La entidad proveerá a todos los funcionarios y contratistas un correo electrónico institucional en el dominio loteriadebogota.com, de acuerdo con las funciones realizadas y a la capacidad de cuentas disponibles apropiadas en la LOTERÍA DE BOGOTÁ.

La cuenta de correo electrónico institucional es personal e intransferible, los usuarios son completamente responsables de todas las actividades realizadas con sus credenciales de acceso y el buzón asociado al correo de la entidad.

El correo electrónico institucional se debe utilizar estrictamente como herramienta de comunicación de la LOTERÍA DE BOGOTÁ, es decir, que debe ser usado para transmitir información relacionada única y exclusivamente con el desarrollo de las funciones misionales y de apoyo asignadas.

Teniendo en cuenta que el correo electrónico institucional es una herramienta para el intercambio de información necesaria que permita el cumplimiento de las funciones propias de cada cargo y no una herramienta de difusión masiva de información, no debe ser utilizada como servicio personal de mensajes o cadenas a familiares o amigos, esquemas piramidales, terrorismo, pornografía, programas piratas, proselitismo político, religioso o racial, amenazas, estafas, virus o código malicioso. Acciones de esta naturaleza se consideran violatorias de las políticas de la entidad y de la ley y serán sancionadas de acuerdo con la Ley 1952 de 2019 “Por el cual se expide el Código General Disciplinario”.

El servidor de correo bloqueará archivos adjuntos o información nociva como archivos .exe o de ejecución de comandos.

Bajo ningún motivo se debe abrir o ejecutar un correo de origen desconocido, debido a que podría tener código malicioso (virus, troyanos, keyloggers, gusanos, etc.), lo cual podría atentar contra los sistemas, programas e información de la LOTERÍA DE BOGOTÁ.

No está permitido abrir, usar o revisar la cuenta de correo electrónico de otro usuario como si fuera propia o suplantándolo. Solamente se podrá acceder al correo electrónico para consulta de otro usuario bajo las siguientes excepciones:

- Los colaboradores con nivel Directivo podrán realizar solicitudes relacionadas con el correo electrónico de colaboradores que están bajo su coordinación o supervisión.
- Que el funcionario que se ausente por enfermedad o vacaciones y la entidad tenga la imperante necesidad de acceder a la información que se encuentre en los dispositivos o correos asignados al colaborador.
- Que el colaborador y la entidad rompan estrepitosamente la relación laboral o contractual y Lotería de Bogotá requiera acceso a la información que se encontraba en poder del colaborador.
- Cuando existan sospechas de espionaje corporativo, de algún acto de corrupción, incidente de seguridad de la información o en general, de alguna actividad delictiva por parte de algún colaborador que pudiera afectar los intereses de la Lotería de Bogotá.
- Para evitar el sabotaje, la modificación o eliminación de la información que se encuentre en poder de algún colaborador, en caso de un eventual conflicto o terminación de la relación laboral o contractual con la entidad.

El usuario debe notificar correos sospechosos a través de la mesa de servicio GLPI o mediante el correo mesadeservicio@loteriadebogota.com, estos correos no deben ser reenviados a ningún usuario, no se deben abrir enlaces, ni abrir los archivos adjuntos que contengan.

El servidor que entre en periodo de vacaciones debe redireccionar su correo electrónico a su jefe inmediato o a quien asignen sus funciones, de no hacerlo la entidad procederá a bloquear dicha cuenta.

5.6. Gestión de medios removibles (unidades de almacenamiento)

La LOTERÍA DE BOGOTÁ promoverá el uso de carpetas compartidas en lugar de medios removibles (USB, discos externos, CD/DVD, entre otros) para el intercambio de información al interior de la entidad.

Las unidades de medios removibles de las estaciones de trabajo, equipos portátiles y servidores se administrarán mediante directorio activo y quien requiera hacer uso de estas unidades debe solicitar la activación la Oficina de Gestión Tecnológica e Innovación, previa autorización del jefe de unidad, indicando el tiempo por el cual se requiere la activación.

Las personas que requieran los medios removibles habilitados de forma permanente deben tener una autorización por el jefe de dependencia y/o área.

La empresa de vigilancia de la entidad, controlará el ingreso y salida de los equipos de cómputo de la entidad.

Los medios removibles en los que se almacene información catalogada como información pública clasificada e información pública reservada deben estar cifrados.

Si ya no se requiere el contenido de un medio reusable, se debe remover de forma que la información no se pueda recuperar, esta actividad será responsabilidad de la Oficina de Gestión Tecnológica e Innovación.

5.7. Clasificación de la información

En atención a los requisitos de la norma NTC-ISO/IEC 27001:2013, la Ley 1712 de 2014 y el Decreto 103 de 2015, la LOTERÍA DE BOGOTÁ clasifica, etiqueta y maneja la información y sus activos asociados de acuerdo con las actividades de Control de Documentos de la LOTERÍA DE BOGOTÁ.

5.7.1. Disposición de los medios

Los medios que contienen información confidencial se deben disponer en forma segura, mediante incineración, destrucción o el borrado de datos antes de ser reutilizados o dados de baja, por la Oficina de Gestión Tecnológica e Innovación.

Todos los Backups se deben cifrar antes de ser entregados a la empresa transportadora.

La información almacenada en medios magnéticos viejos debe ser transferida a medios nuevos antes de que se vuelvan ilegibles, de acuerdo con el tiempo de vida útil de los mismos.

5.7.2. Transferencia de medios físicos

Para la transferencia de medios físicos se deben seguir las directrices del proceso usado para realizar el Control de Documentos de la LOTERÍA DE BOGOTÁ, así como los documentos relacionados.

5.8. CONTROL DE ACCESO

5.8.1. Política de control de acceso a los sistemas de información.

La Oficina de Gestión Tecnológica e Innovación controlará el acceso mediante el enfoque basado en roles, aplicando los siguientes principios.

Lo que necesita conocer: solamente se concede acceso a la información que la persona necesita para la realización de sus tareas (diferentes tareas/roles significan diferentes cosas que se necesita saber y, en consecuencia, diferentes perfiles de acceso).

Lo que necesita usar: solamente se concede acceso a las instalaciones de procesamiento de información (equipos de TI, aplicaciones, procedimientos, recintos) que la persona necesita para la realización de su tarea/trabajo/rol.

5.8.2. Acceso a redes y a servicios en red

Ningún funcionario o contratista podrá compartir archivos o carpetas de un equipo de cómputo a otro sin la respectiva autorización de la Oficina de Gestión Tecnológica e Innovación y del jefe inmediato o supervisor.

El acceso a redes Wifi se controla con autenticación por contraseña utilizando el protocolo WPA2-PSK o el portal cautivo.

La Oficina de Gestión Tecnológica e Innovación proporciona un servicio de conectividad a todos los servidores, contratistas, proveedores y visitantes de la entidad para la navegación en internet, la cual es controlada mediante perfiles de navegación.

La conexión remota a la red de área local de la LOTERÍA DE BOGOTÁ, debe ser

realizada a través de una conexión VPN segura o mediante conexión de acceso remoto, suministrada por la Oficina de Gestión Tecnológica e Innovación, previa autorización del jefe de unidad o líder de proceso quien será el encargado de realizar la solicitud formal a la Oficina de Gestión Tecnológica e Innovación.

5.8.3. Gestión de acceso de usuarios

El acceso a usuarios, la gestión de derechos de acceso privilegiado, la gestión de información de autenticación secreta, retiro o ajuste a los derechos de acceso se realizan de acuerdo a la solicitud previamente enviada por recursos humanos o Jefes de Unidad o líderes de procesos al correo mesadeservicio@loteríadebogotá.com.

5.8.4. Uso de Información de autenticación secreta (Responsabilidades de los Usuarios)

Cada usuario es responsable de mantener a salvo la contraseña de ingreso al equipo. Adicionalmente, los usuarios autorizados a acceder a los sistemas de información de la LOTERÍA DE BOGOTÁ, son responsables de la seguridad de las contraseñas y cuentas de usuario. Cabe resaltar que las contraseñas son únicas e intransferibles.

No se deberá guardar o escribir las contraseñas en papeles físicos o documentos de texto como bloc de notas, Word o las notas de Windows.

La contraseña escogida para el acceso a cada uno de los sistemas de información de la LOTERÍA DE BOGOTÁ debe:

Ser diferente para cada aplicación o sistema de información con excepción de

aquellos sistemas que se autentiquen contra el directorio activo.

No debe contener características personales o de los parientes tales como nombres, apellidos, fechas de cumpleaños o alguna otra fecha importante.

No debe contener palabras de diccionario. Las palabras en idioma inglés y español son las primeras utilizadas por los atacantes.

Las contraseñas se deben establecer teniendo en cuenta los siguientes parámetros: Deben contener mayúsculas, minúsculas, números, caracteres especiales y mínimo ocho (8) caracteres. Las contraseñas deben ser cambiadas cada cuarenta y cinco (45) días. Para ello, las aplicaciones controladas mediante el directorio activo al igual que el correo electrónico, exigirán el cambio automático de las contraseñas con la periodicidad mencionada, las contraseñas del sistema administrativo y financiero deben ser actualizadas por el usuario.

Está prohibido facilitar o proporcionar acceso a las aplicaciones e información a usuarios o a terceros no autorizados.
Para desbloquear la clave de acceso a los diferentes sistemas de información, el usuario debe realizar la solicitud ante la mesa de servicio a través del correo mesadeservicio@loteriadebogota.com.

5.8.5. Control de acceso a sistemas y aplicaciones

El control de acceso a sistemas y aplicaciones se establece de acuerdo al rol del usuario y sus funciones en la entidad, el jefe inmediato debe enviar por correo la solicitud a través de la mesa de servicio - mesadeservicio@loteriadebogota.com.

Con el fin de controlar el acceso no autorizado a sistemas y aplicaciones, las contraseñas de cuentas de administración genéricas (root, SYS, SYSADMIN, cuenta de administrador de Windows, entre otras) deben ser cambiadas anualmente o cada vez que expire el tiempo.

La Oficina de Gestión Tecnológica e Innovación debe cambiar las contraseñas por defecto (y donde sea posible, los usuarios por defecto) de las aplicaciones y servicios utilizados por la LOTERÍA DE BOGOTÁ.

El uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones, no están permitidos para fines diferentes a las actividades propias de la Oficina de Gestión Tecnológica e Innovación.

5.9. CONTROLES CRIPTOGRÁFICOS

La Oficina de Gestión Tecnológica e Innovación debe determinar los algoritmos criptográficos y protocolos autorizados para su uso en la entidad y configurar los sistemas para permitir únicamente aquellos algoritmos autorizados, teniendo en cuenta la información de los grupos de interés con el fin de descartar algoritmos de cifrados débiles tales como DES, RC3, RC4 y protocolos débiles tales como SSLv2 y SSLv3. Se debe considerar en su lugar el uso de algoritmos tales como AES (cifrado simétrico), RSA (cifrado asimétrico) y los protocolos SSL/TLS 1.2 o 1.3 y tamaños de cifrado de 168 o 256 bits (cifrado simétrico) y 2048 bits (cifrado asimétrico) preferiblemente en el caso de ser requeridos.

Las llaves criptográficas deben ser cambiadas anualmente o cada vez que se sospeche que han perdido su confidencialidad.

La administración de tokens bancarios, tokens para acceso a sistemas de

información de entes de control y firmas digitales, estarán a cargo de cada uno de los funcionarios o contratistas a quienes les fueron asignados para el desempeño de sus funciones y/u obligaciones.

Los tokens bancarios y tokens de acceso sistemas de información de entes de control y firmas digitales, deben estar almacenados bajo llave cuando no los están utilizando o cuando se van a retirar de sus puestos de trabajo.

5.10. SEGURIDAD FÍSICA Y DEL ENTORNO

5.10.1. Áreas seguras

La LOTERÍA DE BOGOTÁ cuenta con los siguientes controles para prevenir el acceso no autorizado a las instalaciones de la entidad.

Sistema de acceso biométrico en la entrada, para servidores y/o contratistas, proveedores o visitantes.

El personal de vigilancia, son los encargados de validar el ingreso de visitantes con el área correspondiente, se registra al visitante (identificación, huella y dependencia a la cual se dirige), en caso de ingresar equipos deben quedar registrados en la minuta respectiva.

Cámaras de seguridad en los pasillos de la LOTERÍA DE BOGOTÁ, monitoreadas todo el tiempo desde la recepción de la entidad.

El Centro de Cómputo de la LOTERÍA DE BOGOTÁ cuenta con sistema de detección y extinción de incendios, aire acondicionado, sistema de alimentación

ininterrumpida (UPS) y corriente regulada.

Las áreas de la LOTERÍA DE BOGOTÁ están delimitadas por una barrera física y el ingreso debe hacerse a través de cualquiera de las dos puertas de acceso controlada por cerraduras.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

El Centro de Cómputo debe contar con mecanismos que garanticen que cumplen los requisitos ambientales (temperatura, humedad, voltaje, entre otros) especificados por los fabricantes de los servidores y equipos de comunicaciones que alberga.

Todo acceso al Centro de Cómputo de la LOTERÍA DE BOGOTÁ, se realizará mediante solicitud enviada al correo mesadeservicio@loteriadebogota.com y tendrá un caso asociado para el respectivo seguimiento y control.

La LOTERÍA DE BOGOTÁ cuenta con un plan de emergencias que es probado anualmente, con el fin de brindar protección contra amenazas externas.

5.10.2. Ubicación y protección de los equipos

El Centro de Cómputo está ubicado en la Oficina de Gestión Tecnológica e Innovación, de forma tal que personas no autorizadas no puedan ver la información durante su uso y el acceso físico es controlado por los funcionarios de la Oficina de Gestión Tecnológica e Innovación.

5.10.3. Servicios de suministro

La entidad cuenta con aire acondicionado, un sistema de alimentación no interrumpida (UPS), que asegura el tiempo necesario para que entre en funcionamiento la planta eléctrica que tiene el edificio, también se tiene un canal dedicado para el acceso a internet con su respectivo canal de backup.

La planta eléctrica suministrar energía a los equipos de cómputo, algunas zonas comunes

5.10.4. Seguridad del cableado

El cableado del Centro de Cómputo de la entidad debe cumplir con la normatividad de cableado estructurado y estar debidamente certificado.

5.10.5. Mantenimiento de equipos

La Oficina de Gestión Tecnológica e Innovación establece, ejecuta (mantenimiento correctivo), subcontrata (mantenimiento preventivo) y hace seguimiento a los planes anuales de mantenimiento de la infraestructura tecnológica de la entidad.

5.10.6. Seguridad de equipos y activos fuera de las instalaciones

La salida de equipos de la entidad es controlada mediante memorando o correo electrónico autorizada por la jefe de la unidad de recursos físicos y/o del Almacén. Esta política aplica para todos los funcionarios y/o contratistas, excepto para el (la) gerente, subgerente y secretario general.

Los medios removibles que son retirados de las instalaciones de la entidad con Backup deben ser debidamente cifrados por la Oficina de Gestión Tecnológica e Innovación.

Los servidores y contratistas que retiren equipos o medios removibles de las instalaciones de la entidad deben seguir las siguientes directrices:

Bajo ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista, en el caso que esté siendo transportado en un vehículo.

Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

En caso de pérdida o robo de un equipo de la entidad, se debe poner la denuncia ante la autoridad competente e informar inmediatamente al Unidad de Recursos Físicos, al responsable del Almacén y al responsable de la Oficina de Gestión Tecnológica e Innovación para que se inicie el trámite interno correspondiente.

5.10.7. Disposición segura o reutilización de equipos

Cuando una estación de trabajo, equipo portátil o medio removible vaya a ser reasignado o dado de baja, se debe realizar una copia de respaldo de la' información de la entidad que allí se encuentre almacenada (en caso de ser necesario).

Posteriormente, el equipo debe ser sometido a un proceso de eliminación segura de la información almacenada (destrucción física, eliminación o sobreescritura de los medios que contienen información) con el fin de evitar pérdida de la información y/o recuperación no autorizada de la misma.

Para el caso de las licencias que se encuentran en físico se destruyen y se deja evidencia y testigos del procedimiento realizado.

5.10.8. Política de equipo desatendido, escritorio limpio y pantalla limpia

Los funcionarios y contratistas de la LOTERÍA DE BOGOTÁ deben conservar su escritorio físico libre de información propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o personal que no tenga autorización para su uso o conocimiento.

Los computadores mostrarán por defecto el fondo y protector de pantalla de la LOTERÍA DE BOGOTÁ; este no podrá ser modificado por ningún usuario y debe permanecer activo.

Los funcionarios y contratistas de la LOTERÍA DE BOGOTÁ deben bloquear la pantalla de su computador cuando por cualquier motivo se ausenten del puesto de trabajo.

Se prohíbe el almacenamiento de información personal en los computadores y servidores de la LOTERÍA DE BOGOTÁ.

El escritorio lógico debe estar libre de información pública clasificada e información

pública reservada

5.11. SEGURIDAD DE LAS OPERACIONES

5.11.1. Documentación de procedimientos operativos

Se debe contar con procedimientos documentados para las actividades operativas asociadas con las instalaciones de procesamiento de información.

5.11.2. Control de cambios

Los cambios en los procesos de negocio serán gestionados por el comité institucional de gestión y desempeño.

Los cambios en la documentación de los procesos se deben realizar siguiendo las actividades que soportan el Control de Documentos.

Los cambios en los sistemas de información se realizan de acuerdo con la solicitud de realizadas por el servidor a través de la mesa de servicio. Mesadeservicio@loteriadebogota.com.

5.11.3. Gestión de capacidad

La entidad gestiona la capacidad de su plataforma tecnológica (hardware y software) de acuerdo con las indicaciones que serán tomadas en la Oficina de Gestión Tecnológica e Innovación.

5.11.4. Separación de los ambientes

La entidad cuenta con ambientes de desarrollo y producción separados por máquinas virtuales.

La entidad controla el acceso al ambiente de desarrollo de la misma forma que controla el acceso al ambiente de producción, siguiendo las directrices de la política de control de acceso.

5.12. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

Se deben proteger las estaciones de trabajo, equipos portátiles y servidores de la entidad contra códigos maliciosos.

Los contratistas que hagan uso de sus equipos portátiles personales deben contar con un software antivirus licenciado.

El servicio de antivirus no requiere de solicitud o autorización para su uso, todos los equipos de la LOTERÍA DE BOGOTÁ conectados a la red deben tener el antivirus instalado y activo.

El único servicio de antivirus autorizado para las estaciones de trabajo y los equipos portátiles de los funcionarios de la LOTERÍA DE BOGOTÁ es el asignado directamente por la Oficina de Gestión Tecnológica e Innovación, el cual cumple con todos los requisitos técnicos y de seguridad requeridos.

El usuario no debe propiciar el intercambio de archivos que hayan sido identificados como infectados por virus o códigos maliciosos o sean sospechosos de estar infectados.

El usuario NO debe instalar o emplear programas no autorizados para manejo de antivirus.
Los usuarios no deben desactivar o eliminar los archivos que forman parte del programa antivirus.

El programa antivirus debe ser instalado única y exclusivamente por la Oficina de Gestión Tecnológica e Innovación, en los servidores, estaciones de trabajo y equipos de cómputo de los funcionarios y contratistas de la LOTERÍA DE BOGOTÁ.

Es deber de los usuarios informar a la Oficina de Gestión Tecnológica e Innovación en caso de que el antivirus no se encuentre activo o este desactualizado.

5.13. COPIAS DE RESPALDO

La entidad debe realizar copias de respaldo de la información y pruebas periódicas a las mismas. Para ello la Oficina de Gestión Tecnológica e Innovación cuenta con actividades para realizar la Gestión de Copias de Seguridad.

La Oficina de Gestión Tecnológica e Innovación establecerá las políticas y estándares de copias de seguridad para los sistemas de información y bases de datos.

Las copias de respaldo se guardarán únicamente con el objetivo de restaurar información cuando por situaciones como borrado de datos, incidente de seguridad de la información, defectos en los discos de almacenamiento, problemas de los servidores o equipos de cómputo, o por requerimientos legales, sea necesario recuperarla.

Los funcionarios y contratistas son responsables de almacenar la información que requiera copias de respaldo, en las carpetas compartidas asignadas por la Oficina de Gestión Tecnológica e Innovación a cada una de las áreas de la LOTERÍA DE BOGOTÁ, dado que la información que se encuentra almacenada en ubicaciones diferentes no será respaldada.

5.14. REGISTRO Y SUPERVISIÓN

5.14.1. Registro de eventos

Los sistemas operativos, servicios y sistemas de información que hacen parte de la infraestructura para el procesamiento de información y comunicaciones de la entidad, deben generar archivos de registro de eventos (logs) definidos en conjunto por los responsables de su administración.

5.14.2. Protección de la información de registro

La Oficina de Gestión Tecnológica e Innovación con el fin de proteger la información de registro de modificación por parte de usuarios no autorizados, administradores u operadores de los sistemas de información, implementará mecanismos de copiado de logs en “tiempo real” a un sistema por fuera del control de administradores y operadores de los sistemas.

5.14.3. Sincronización de relojes

Con el fin de obtener un control apropiado para la relación adecuada de eventos no deseados en la infraestructura o para la investigación efectiva de incidentes, los relojes de los diferentes equipos de cómputo, servidores y sistemas de información utilizados por la LOTERÍA DE BOGOTÁ, deberán estar sincronizados por el servidor

de dominio.

5.15. CONTROL DE SOFTWARE OPERACIONAL

5.15.1. Instalación de software en sistemas operativos

El proceso de instalación y desinstalación de software está autorizado exclusivamente al personal de la Oficina de Gestión Tecnológica e Innovación. Por lo tanto, a cualquier otro servidor público o contratista no le es permitido realizar esta labor.

Para la instalación de software se tendrán en cuenta las siguientes directrices por la Oficina de Gestión Tecnológica e Innovación y únicamente es esta Área la que podrá hacer cualquier instalación:

El software propietario debe contar con su respectiva licencia y en el caso del software libre debe estar permitido el uso comercial.

El instalador debe ser descargado de la página oficial del fabricante.

Debe verificarse la integridad del archivo por medio de la comprobación de códigos hash (siempre que el fabricante proporcione esta información).

Ningún usuario se encuentra autorizado para instalar aplicaciones o software en los

equipos de Cómputo de la Lotería de Bogotá

Se debe proporcionar capacitación adecuada a los usuarios y al personal técnico en los aspectos de operación y funcionalidad de los nuevos sistemas de información o mejoras a sistemas de información existentes, antes de su puesta en marcha.

Todos los sistemas nuevos y mejorados deben estar completamente soportados por una documentación suficientemente amplia y actualizada, y no deben ser puestos en el ambiente de producción sin contar con la documentación disponible.

5.16. GESTIÓN DE LA VULNERABILIDAD TÉCNICA

5.16.1. Gestión de las vulnerabilidades técnicas

La Oficina de Gestión Tecnológica e Innovación, es responsable de verificar de manera periódica (al menos semestralmente) la información publicada por parte de los fabricantes y foros de seguridad en relación con nuevas vulnerabilidades identificadas que puedan afectar los sistemas de información de la entidad.

Se debe generar y ejecutar por lo menos una vez al año un plan de análisis de vulnerabilidades y/o hacking ético para las plataformas críticas de la LOTERÍA DE BOGOTÁ, cuya viabilidad técnica y de administración lo permita.

5.17. CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN

5.17.1. Controles sobre auditorías de sistemas de información

Para la ejecución de auditorías a los sistemas de información se deben tener en

cuenta las siguientes consideraciones:

- Los requisitos de auditoría para acceso a sistemas y a datos se deben acordar con el jefe de área y/o dependencia involucrada.
- El alcance de las pruebas técnicas de auditoría se debe acordar y controlar.
- Las pruebas de auditoría (incluidas las pruebas de análisis de vulnerabilidades y/o hacking ético) que puedan afectar la disponibilidad del sistemase deben realizar fuera de horas laborales.
- Se debe hacer seguimiento de todos los accesos y logs para producir un rastro de referencia.

5.18. SEGURIDAD EN LAS COMUNICACIONES

5.18.1. Gestión de la seguridad en las redes

La Oficina de Gestión Tecnológica e Innovación debe definir e implementar los mecanismos de control que considere apropiados para proteger la confidencialidad, integridad y disponibilidad de las redes, los servicios en red y la información por allí transmitida.

La Oficina de Gestión Tecnológica e Innovación definirá e implementará los mecanismos de separación de las redes de la LOTERÍA DE BOGOTÁ con base en los niveles de confianza (por ejemplo, dominio de acceso público, dominio de acceso interno)

El acceso remoto a las redes de la entidad se controla mediante conexiones VPN.

5.18.2. Transferencia de información

La entidad incluye una cláusula de confidencialidad en los contratos con terceros

que tengan acceso a la información y que por alguna razón requieran conocer o intercambiar información restringida o confidencial. En este acuerdo quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se firmarán antes de permitir el acceso o uso de dicha información.

Los servidores y contratistas deben seguir las indicaciones de gestión documental para la transferencia de información, siguiendo los parámetros de la clasificación de la información de acuerdo con las tablas de retención documental - TRD de la LOTERÍA DE BOGOTÁ.

5.19. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

5.19.1. Requisitos de seguridad de los sistemas de información

La Oficina de Gestión Tecnológica e Innovación debe definir los requisitos de seguridad de la información para sistemas de información nuevos o mejoras a los sistemas de información existentes, contratados externamente o desarrollados en la entidad. Para ello, deben tener en cuenta:

- El nivel de confianza requerido con relación a la identificación declarada delos usuarios, para obtener los requisitos de autenticación de usuario. Por ejemplo, la implementación de segundos factores de autenticación y un sistema de gestiónde contraseñas que exija el uso de contraseñas fuertes, el cambio periódico de contraseñas y que guarde un historial de contraseñas para evitar de nuevo su uso.

- Los procesos de suministro de acceso y de autorización para usuarios, al

igual que para usuarios privilegiados o técnicos. Por ejemplo, el suministro de datosde acceso por correo electrónico.

- Las necesidades de protección de activos involucrados, en particularacerca de disponibilidad, confidencialidad e integridad. Por ejemplo, cifrado de información almacenada, el envío de información por canales cifrados.

- Los requisitos obtenidos de los procesos del negocio, tales como los requisitos de ingreso, seguimiento, y no repudio, formularios de autenticación mediante HTTPS, cifrado de contraseñas almacenadas y uso de firmas digitales.

- Los requisitos de trazabilidad (registro de eventos) de las actividades de los usuarios.

- La necesidad de exigir la implementación de metodologías de desarrollo seguro.

Todos los desarrollos o adquisición de software de terceros, deben ser gestionados por la Oficina de Gestión Tecnológica e Innovación con el fin verificar requisitos técnicos y seguridad de la información.

5.19.2. Seguridad en los procesos de desarrollo y soporte

5.19.2.1. Política de desarrollo seguro

La entidad velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requisitos de seguridad, así como con pruebas de aceptación y seguridad al software desarrollado. Además, la entidad asegurará que

todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la entidad.

5.19.2.2. Cambios en sistemas, plataforma tecnológica o paquetes de software

Los cambios en sistemas deben llevarse a cabo de acuerdo con el procedimiento Gestión del Cambio.

5.19.2.3. Principios de desarrollo seguro

La Oficina de Gestión Tecnológica e Innovación debe definir e implementar principios de desarrollo seguro en actividades de construcción de sistemas de información internos.

Los principios de desarrollo establecidos se deben revisar con regularidad (al menos anualmente) para asegurar que están contribuyendo a mejorar los estándares de seguridad dentro del proceso de desarrollo y asegurar que permanezcan actualizados en términos de combatir nuevas amenazas potenciales y seguir siendo aplicables a los avances en las tecnologías y soluciones que se aplican.

Los datos de configuración del sistema como, por ejemplo: contraseñas, direcciones IP, datos de conexión a bases de datos y otros parámetros de configuración deben quedar almacenadas en archivos o bases de datos cifradas. Está prohibida la inclusión de estos parámetros en el código fuente.

5.19.2.4. Ambiente de desarrollo seguro

La Oficina de Gestión Tecnológica e Innovación aplicará los mismos controles

aplicados al ambiente de producción en el ambiente de pruebas, tales como, control de acceso, copias de respaldo, registro de eventos y separación de ambientes (desarrollo y producción).

La Oficina de Gestión Tecnológica e Innovación debe implementar los controles necesarios para asegurar que las migraciones entre los ambientes de pruebas y producción han sido aprobadas, de acuerdo con las actividades para gestionar cambios de seguridad de la información.

La Oficina de Gestión Tecnológica e Innovación debe contar con sistemas de control de versiones para administrar los cambios en los sistemas de información desarrollados al interior de la entidad.

5.19.2.5. Desarrollo contratado externamente

La Oficina de Gestión Tecnológica e Innovación debe asegurase que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento en el cual se especifiquen las condiciones de uso del software y los derechos de propiedad intelectual.

Las áreas y/o dependencias deben exigir el suministro de evidencia que se realizaron pruebas de seguridad al software desarrollado por terceros.

Los principios de desarrollo seguro se deben aplicar, en donde sea pertinente, a desarrollos contratados externamente.

Las áreas y/o dependencias que contraten desarrollos externos deben asegurar que se realicen pruebas de aceptación del software, con el fin de verificar el cumplimiento de los requisitos de seguridad acordados.

Las áreas y/o dependencias deben tener en cuenta e incluir en los acuerdos contractuales la necesidad de que el software cumpla con las leyes y regulaciones aplicables.

Las áreas y/o dependencias deben incluir en acuerdos contractuales, en donde sea posible, el derecho de la entidad a realizar auditorías durante el desarrollo del contrato.

Cuando se contrata un desarrollo externo se debe acordar el cumplimiento de los niveles de soporte requeridos por la entidad. Adicionalmente, se debe acordar la entrega de manual(es) técnico(s), que describa(n) la estructura interna del sistema, así como el diccionario de datos, librerías y archivos que lo conforman; y manual(es) funcional(es), que describa(n) las funcionalidades de cada una de las opciones del menú de la aplicación.

5.19.2.6. Pruebas de seguridad de sistemas

Se debe contar tanto para desarrollos internos como externos con la ejecución de pruebas funcionales que incluyan la evaluación de los requisitos de seguridad de la información y la protección contra vulnerabilidades conocidas.

5.19.2.7. Pruebas de aceptación de sistemas

Se deben realizar pruebas de aceptación del software, independientemente de que sea un desarrollo interno o un desarrollo contratado externamente, con el fin de validar los requisitos de seguridad de la información y la adherencia a prácticas de desarrollo de sistemas seguros (en donde sea aplicable).

En estas pruebas se puede hacer uso de herramientas automatizadas, tales como herramientas de análisis de códigos o escáneres de vulnerabilidad, y se debe verificar que se han corregido los defectos relacionados con la seguridad.

De ser posible, las pruebas de aceptación se deben llevar a cabo en un ambiente de pruebas realista, para asegurar que el sistema no introducirá vulnerabilidades al ambiente de la entidad, y que las pruebas son confiables.

5.19.2.8. Datos de prueba

La Oficina de Gestión Tecnológica e Innovación debe certificar que la información a ser entregada a los desarrolladores (tanto internos como externos) para sus pruebas será enmascarada o que los datos sensibles serán eliminados con el fin de no revelar información confidencial de los ambientes de producción y, por ende, dar cumplimiento a la Ley 1581 de 2012 (Ley de Protección de Datos Personales) y la Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información pública).

5.20. RELACIÓN CON LOS PROVEEDORES

5.20.1.1. Seguridad de la información en las relaciones con los proveedores

5.20.1.1.1. Política de seguridad de la Información para las relaciones con proveedores

La LOTERÍA DE BOGOTÁ establecerá mecanismos de control en sus relaciones con proveedores, con el objetivo de asegurar la información a la que tengan acceso o servicios que sean provistos por los mismos, y que se cumpla con las políticas de

la entidad.

5.20.1.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores

Los supervisores de contratos se asegurarán de comunicar las políticas y procedimientos a los proveedores y/o contratistas.

Se deben incluir en los acuerdos con proveedores y/o contratistas, como mínimo, los siguientes requisitos de seguridad de la información:

- Cláusula de confidencialidad.
- Cláusula de protección de datos personales.
- Cláusula que defina las responsabilidades que continúan después de terminado el contrato (por ejemplo, confidencialidad durante 5 años después de terminado el contrato).

Cumplimiento de las políticas de seguridad de la información de la LOTERÍA DE BOGOTÁ.

Acciones para tomar en caso de incumplimiento de las políticas de seguridad de la información.

Reporte de eventos de seguridad de la información a través de la mesadeservicio@loteriadebogota.com.

Cláusula de seguimiento y revisión de los servicios prestados por los proveedores y/o contratistas para asegurar que los términos y condiciones de seguridad de la información de los acuerdos se cumplan.

Responsabilidades de los proveedores incluidos en la cadena de suministro, tales como, soporte técnico y garantía.

Los supervisores de contratos deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad de la información establecidos con ellos, y monitoreando la aparición de nuevos riesgos.

Los accesos a los sistemas de información y equipos de cómputo requeridos por los proveedores deben ser solicitados de manera formal a la Oficina de Gestión Tecnológica e Innovación a través de la mesa de servicios mesadeservicio@loteriadebogota.com.

5.21. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La entidad realizará el seguimiento a los incidentes de seguridad de la información de acuerdo con las directrices del procedimiento Gestión de Incidentes de Seguridad de la Información.

5.22. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

5.22.1. Continuidad de la seguridad de la información

La entidad planificará e implementará la continuidad del negocio (PCN) teniendo en cuenta el talento humano, recursos tecnológicos, activos de información y los procesos críticos de la entidad, además de la continuidad de la seguridad de la información.

La entidad realizará pruebas periódicas (al menos anualmente) al plan de continuidad del negocio y de continuidad de la seguridad de la información implementados, con el fin de asegurar que serán válidos y eficaces durante situaciones adversas.

5.22.2. Redundancias

La entidad establecerá e implementará un Plan de Recuperación de Desastres (PRD) como parte del Plan de Continuidad de Negocio (PCN) con el fin de asegurar la redundancia y continuidad de las instalaciones de procesamiento de información.

La entidad realizará pruebas periódicas (al menos anualmente) al PRD, con el fin de asegurar que los controles tecnológicos implementados serán válidos y eficaces durante situaciones adversas.

5.23. CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

5.23.1. Identificación de la legislación aplicable y de los requisitos contractuales

La Secretaría General y el Oficial de Seguridad deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la entidad que están relacionados con seguridad de información. Para ello, se pueden apoyar en el Comité Institucional de Gestión y Desempeño.

5.23.2. Derechos de propiedad intelectual

La Oficina de Gestión Tecnológica e Innovación realizará revisiones periódicas (al

menos semestralmente), con el fin de asegurar que todo el software que se ejecute en la entidad esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.

Los usuarios no deben instalar software o sistemas de información en sus estaciones de trabajo o equipos portátiles suministrados para el desarrollo de sus funciones.

Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, La Oficina de Gestión Tecnológica e Innovación podrá distribuir un número de copias de software bajo una licencia otorgada.

Los supervisores de contratos deben asegurarse de incluir cláusulas de propiedad intelectual y derechos de autor en contratos con terceros.

5.23.3. Protección de registros

La LOTERÍA DE BOGOTÁ se obliga a proteger todos los registros que muestren evidencia del cumplimiento de los requisitos normativos, legales o regulatorios contra la pérdida de confidencialidad, disponibilidad e integridad, siguiendo las directrices de los activos de información.

5.23.4. Privacidad y protección de información de datos personales

La LOTERÍA DE BOGOTÁ, quien será responsable del tratamiento de los Datos Personales, tal y como este término se define en la Ley 1581 de 2012, respeta la

privacidad de cada uno de los terceros que le suministren sus datos personales a través de los diferentes puntos de recolección y captura de dicha información. Por lo tanto, la entidad implementará los controles necesarios para su protección y en ningún momento divulgará esta información a terceras partes a menos que cuente con la autorización formal de los mismos o en los casos en que la ley lo permita.

5.23.5. Reglamentación de controles criptográficos

La LOTERÍA DE BOGOTÁ, se regirá por la Ley 527 de 1999 (acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y otras disposiciones) y sus decretos reglamentarios, según se requiera.

5.24. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

5.24.1. Revisión independiente de la seguridad de la información

La Oficina de Control Interno realizará auditorías internas de revisión al menos una vez al año, siguiendo las directrices del procedimiento de Auditorías Internas al Sistema Integrado de Gestión. Esta revisión independiente es necesaria para asegurar la conveniencia, la adecuación y la eficacia continuas del enfoque de la entidad para gestionar la seguridad de la información.

5.24.2. Cumplimiento con las políticas y normas de seguridad

Los jefes de unidad y/o dependencia deben revisar con regularidad (al menos una vez por año) el cumplimiento de las políticas y procedimientos de seguridad de la información dentro de su área de responsabilidad.

5.24.3. Revisión del cumplimiento técnico

La Oficina de Gestión Tecnológica e Innovación debe coordinar la revisión periódica (al menos anualmente) de los sistemas de información utilizados en la LOTERÍA DE BOGOTÁ, para determinar el cumplimiento con las políticas y procedimientos de seguridad de la información. Para ello, se debe determinar a qué sistemas de información se hará revisión cada vez.

5.24.4. Medidas a Adoptar en Caso de Incumplimiento

El incumplimiento de una o más políticas descritas en este documento, está sujeto a las sanciones disciplinarias, fiscales y penales que se deriven de la conducta del implicado, incluso cuando se encuentre en situaciones administrativas como permisos, licencias, vacaciones, suspensiones en ejercicio del empleo o en comisión, de acuerdo con la Ley 734 de 2002, la Ley 906 de 2004 y la Ley 1273 de 2009.

6. NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Toda violación de estas políticas se debe notificar a la Oficina de Gestión Tecnológica e Innovación a través de correo electrónico mesadeservicio@loteriadebogota.com

Asimismo, se deben notificar situaciones tales como: personas ajenas a la LOTERÍA DE BOGOTÁ sin identificación y sin acompañamiento en las oficinas, correos

maliciosos o sospechosos, uso de software ilegal, divulgación, alteración yrobo de información.

7. VIGENCIA

El presente manual entrará en vigencia a partir de la fecha de aprobación, la cual se realizó en sesión del Comité Institucional de Gestión y Desempeño del 28 de abril de 2023.

8. BIBLIOGRAFÍA

ICONTEC. (2013). *Norma Técnica ntc-iso/iec Colombiana 27001*. Colombia.

ISO/IEC. (2012). *NTC-ISO/IEC 27032, Information technology - Security techniques - Guidelines forcybersecurity*.

ISO/IEC. (2018a). *NTC-ISO/IEC 27000, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Visión General y Vocabulario*. *2018*, 1–38. Retrieved from http://k504.khai.edu/attachments/article/819/ISO_27000_2014.pdf

ISO/IEC. (2018b). *NTC-ISO/IEC 27005, Tecnología de la Información. Tecnicas de Seguridad.Gestión del Riesgo en Seguridad de la Información.* (Vol. 2018).

ISO/IEC. (2018c). *NTC-ISO/IEC 31000, Gestión del Riesgo. Directrices*. *2018*, 1–30.

OWASP PROJECT. (2019). SQL Injection - OWASP. Retrieved December 9, 2019, fromhttps://www.owasp.org/index.php/SQL_Injection

Control de Cambios		
FECHA	**DESCRIPCIÓN Y JUSTIFICACIÓN DEL CAMBIO**	**VERSIÓN**
11/01/2019	Se crea el manual PSI y es aprobado.	1
30/07/2021	Se actualiza el manual PSI y se aprueba en el comité institucional de gestión y desempeño del 30 de julio de 2021.	2
28/04/2023	Se actualiza el numeral 5.5.7 Correo electrónico institucional. Se ajusta el nombre a *"POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD DE LA INFORMACIÓN".* Se ajusta el año en la portada y la numeración en la tabla de contenido. Se ajusta el pie de página a GESTIÓN TECNOLÓGICA E INNOVACIÓN.	3
16/08/2023	Se adicionan los siguientes párrafos en los numerales: 5.10.7 Para el caso de las licencias que se encuentran en físico se destruyen y se deja evidencia y testigos del procedimiento realizado. 5.15.1 Ningún usuario se encuentra autorizado para instalar aplicaciones o software en los equipos de Cómputo de la Lotería de Bogotá 5.19.2.3 Los datos de configuración del sistema como, por ejemplo: contraseñas, direcciones IP, datos de conexión a bases de datos y otros parámetros de configuración deben quedar almacenadas en archivos o bases de datos cifradas. Está prohibida la inclusión de estos parámetros en el código fuente. Se reemplaza el término *"Área de Sistemas"* por *"Oficina de Gestión Tecnológica e Innovación"*	4

Control de revisión y aprobación		
ELABORACIÓN	**REVISIÓN**	**APROBACIÓN**
Yolanda Gallego Francisco Daza	Oficina de Planeación Estratégica	Comité Institucional de Gestión y Desempeño 16/08/2023

ANEXO 1.

- **Activo**: Según la norma ISO 27000, es cualquier cosa (información en el caso de ser un activo de información) que tiene valor para un individuo, organizacióno gobierno (ISO/IEC, 2018a).

- **Activo Físico:** Activo que tiene una existencia tangible o material (ISO/IEC, 2012).

- **Activo de Información:** Otro de los conceptos importantes para el desarrollo del presente Manual de políticas de seguridad de la información y es definido por la norma ISO 27000 como el conocimiento o datos que tienen valor para un individuo u organización (ISO/IEC, 2018a).

- **Activos de Seguridad de la Información**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (hardware, software, información física o digital, personas), que tenga valor para la entidad.

- **Amenaza**: Se define como la causa potencial de un incidente no deseado, el cual puede resultar en el daño de un sistema, individuo u organización (ISO/IEC, 2018a).

- **Antivirus**: Programa especializado en la detección y, si es posible, en el bloqueo y/o eliminación de virus informáticos.

- **Aplicación**: La norma ISO 27032 la define como una solución deInfraestructura Tecnológica (IT), que incluye software de aplicación, datos de aplicación y

procedimientos diseñados para ayudar a los usuarios de una organización a desempeñar tareas específicas o gestionar problemas específicos de IT, automatizando funciones o procesos de negocio (ISO/IEC, 2012).

- **Ataque**: Es el intento de destrucción, exposición, interacción, des habilitación, robo u obtención de acceso no autorizado para hacer uso no autorizado de un activo (ISO/IEC, 2018a).

- **Autenticación**: Servicio que permite verificar la identidad de un ciudadano para acceder a trámites y servicios que requieran, a través de medios electrónicos.

- **Backup**: Copia de seguridad de los datos, de tal forma que se pueda restaurar un sistema después de una pérdida de información. Se puede realizar en medios magnéticos, servidores externos y almacenar en un lugar seguro.

- **Borrado seguro**: Proceso de sobreescritura de información en un disco duro u otro medio de almacenamiento informático, que hace que la recuperación delos datos residuales sea una tarea prácticamente imposible.

- **Ciberespacio**: La norma ISO 27032 hace referencia a un ambiente complejo resultante de la interacción de personas, software y servicios en el internet a través de medios de dispositivos tecnológicos y redes conectadas a ellos, los cuales no existen en una forma física (ISO/IEC, 2012).

- **Cifrar**: Es el proceso para volver ilegible información considerada importante. Se trata de una medida de seguridad usada para almacenar o transferir información delicada que no debería ser accesible a terceros. La información una vez cifrada sólo puede leerse aplicándole una clave.

- **Confidencialidad**: La información debe ser accesible sólo a aquellas personas autorizadas.

- **Control – Contramedida:** Así mismo se define en la norma ISO 27032 como los medios para gestionar el riesgo incluyendo políticas, procedimientos, guías, prácticas o estructuras organizacionales que pueden ser administrativos, técnicos, gerenciales o legales dependiendo de su naturaleza (ISO/IEC, 2012).

- **Criptografía:** Técnica o conjunto de métodos cuya función es transformar un determinado mensaje o información en otro totalmente distinto ilegible para aquellas personas que no estén autorizadas a leerlo.

- **Disponibilidad**: La información y los servicios deben estar disponible cuando se le requiera.

- **Hardware**: Es un término genérico para todos los componentes físicos de un dispositivo.

- **Incidente**: Un evento o serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Integridad**: La información y sus métodos de procesamiento deben ser completos y exactos.

- **Información**: Datos relacionados que tienen valor para la entidad. La

información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada (ISO/IEC 27001:2013)

- **Información pública:** Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad (Guía No. 5. Guía para la Gestión y Clasificación de Activos - MinTIC).

- **Información pública clasificada:** Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario (Guía No. 5. Guía para la Gestión y Clasificación de Activos - MinTIC)

- **Información pública reservada:** Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica (Guía No. 5. Guía para la Gestión y Clasificación de Activos - MinTIC).

- **Infraestructura Tecnológica:** La infraestructura tecnológica se encuentra integrada por un conjunto de elementos de hardware (servidores, puestos de trabajo, redes, enlaces de telecomunicaciones, etc.), software (sistemas operativos, bases de datos, lenguajes de programación, herramientas de

administración, etc.) y servicios (soporte técnico, seguros, comunicaciones, etc.) que en conjunto dan soporte a las aplicaciones (sistemas informáticos) de una empresa.

- **Keylogger (Registrador de teclas):** Es una herramienta maliciosa que se encarga de registrar las pulsaciones que se hacen sobre el teclado con el fin de capturar lo digitado.

- **Logs de auditoría o registros de eventos**: Registro de eventos almacenados en un archivo, que contiene información relevante de las actividades realizadas sobre sistemas y aplicaciones informáticas. Los logs de auditoría son elprincipal instrumento para detectar, diagnosticar, auditar y analizar problemasde todo tipo, especialmente aquellos que tienen que ver con la seguridad de los datos, de la red, el uso del servicio de navegación en Internet, los errores de las máquinas centrales (Servidores), periféricos, etc.

- **Malware**: Software diseñado con intenciones maliciosas y que contienen características o capacidades que pueden causar un daño potencial directa o indirectamente al usuario y/o a el sistema del computador del usuario (ISO/IEC, 2012).

- **Pendrive usb:** Es un tipo de dispositivo de almacenamiento de datos que utiliza memoria flash para guardar información.

- **Plan de contingencia**: Es un conjunto de procedimientos alternativos a la operatividad normal de cada entidad. Su finalidad es la de permitir el funcionamiento de ésta, aun cuando alguna de sus funciones deje de hacerlo a causa de algún incidente tanto interno como externo a la organización.

- **Programas utilitarios:** Hacen referencia a software diseñado para realizar una función determinada. El término utilitario se refiere normalmente al software que resuelve problemas relacionados con la administración del sistema. Algunos ejemplos de software utilitario son: aplicaciones para cifrado y descifrado de archivos, aplicaciones para compresión de archivos, software antivirus, navegadores (Google Chrome, Mozilla Firefox, entre otros) editores de texto, administradores de tareas, aplicaciones para realizar copias de respaldo, entre otros.

- **Programas utilitarios privilegiados**: Los programas utilitarios privilegiados son aquellos que tienen la capacidad de anular el sistema y los controles de las aplicaciones. Algunos ejemplos son: Interfaz de línea de comandos (cmd en Windows o terminal en linux), administrador de tareas, sniffers de red (wireshark, bettercap, entre otros), herramientas de administración de red.

- **Proyecto**: Planes de trabajo con acciones sistemáticas, planteados por las diferentes áreas de la LOTERÍA DE BOGOTÁ en busca de alcanzar los objetivos de la entidad, que requieren una asignación presupuestal, se rigen por el manual de contratación, manteniendo el adecuado manejo de la información.

- **Riesgo**: Una buena definición al respecto al ámbito de la seguridad de la información corresponde a un “potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando dañoa la organización” (ISO/IEC, 2009, p. 9), sin embargo, una definición un poco más general al respecto es el “efecto de la incertidumbre sobre los objetivos” (ISO/IEC, 2018b, p. 11).

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

- **Sistema de Información:** Conjunto de programas informáticos diseñados y desarrollados con el fin de solucionarnecesidades informáticas.

- **Soporte:** Servicios que proporciona asistencia en los equipos de cómputo, sistemas de información, o algún otro dispositivo electrónico o mecanismo.

- **Spyware**: Software engañoso que recolecta información privada o confidencial del computador de un usuario (ISO/IEC, 2012).

- **Troyano**: Es un programa malicioso capaz de alojarse en un computador y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de apoderarse de la información o controlar remotamente a la máquina.

- **Usuario Final:** Son todos los clientes internos y/o externos que requieren de una funcionalidad mediante la actualización, mejoramiento o adquisición de un sistema de información.

- **VPN**: En informática, acrónimo del Ingles Virtual Prívate Networks, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada.

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