Manual de Políticas de Seguridad de la Información

Lotería de Medellín

TABLA DE CONTENIDO

1. Introducción

La información es un activo esencial para las actividades de las empresas, y en consecuencia necesita una protección adecuada. La seguridad de la información tiene como fin la protección de la información y de los sistemas que la soportan, frente a un gran número y variedad de amenazas y vulnerabilidades.

Para lograr el objetivo de proteger la Información de la Entidad, es necesario implementar un Sistema de Gestión de Seguridad de la Información que incluya: Políticas de Seguridad alineadas al negocio, control de activos asociados a la seguridad, dispositivos de software y hardware, seguridad de los recursos humanos, seguridad física y ambiental, gestión de las comunicaciones, gestión de la continuidad del negocio, entre otros.

En el presente documento se describen las Políticas y Normas de Seguridad de la Información definidas por Lotería de Medellín. Para su elaboración se toman como base los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información del gobierno nacional, el cual se basa a su vez en la norma ISO 27001:2013 y en la Ley 1581 de 2015.

La Seguridad de la Información es una prioridad para la Entidad, por lo tanto es responsabilidad de todos velar para que no se realicen actividades que contradigan la esencia y el objetivo de cada una de las Políticas que se describen en el presente documento.

2. Justificación

Las entidades públicas están obligadas a disponer de un conjunto de políticas de seguridad de la información que sirvan como carta de navegación en lo relacionado con los controles que se deben implementar para garantizar altos niveles de seguridad y privacidad de la información que se gestiona a través de sus sistemas de información.

Teniendo en cuenta que la información es uno de los principales activos de la entidad, la seguridad de la información es una prioridad para Lotería de Medellín y por tanto es responsabilidad de todos sus miembros velar por su cumplimiento, de tal manera que se eviten al máximo prácticas que contradigan la esencia de cada una de estas políticas.

3. Alcance

Las Políticas de Seguridad de la Información cubren los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros que laboren o tengan relación con Lotería de Medellín.

4. Objetivo general

Establecer las Políticas en Seguridad de la Información de la Lotería de Medellín, mediante confidencialidad, disponibilidad, integridad, autenticidad y no repudio de la información que se produce y/o consume a su interior. A través de la construcción de medidas de índole técnica y organizativas necesarias para garantizar la seguridad de la información, basándose en una arquitectura empresarial que apoye de manera permanente al logro de los objetivos estratégicos para fortalecer la gestión institucional.

5. Público objetivo

Todos los miembros de Lotería de Medellín.

6. Marco Legal

Norma	Objeto
Ley 23 de 1982	Sobre derechos de autor
Constitución política de Colombia de 1991. Artículo 15	Habeas data
Ley 594 de 2000	Ley General de archivos
Ley 962 de 2005. Artículo 6	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
Ley 1032 de 2006	Por la cual se modifican los

Norma	Objeto
	artículos 257, 271, 272 y 306 del Código Penal
Ley 1273 de 2009	De la Protección de la información y de los datos
Ley 1437 de 2011. Artículos 58 y 59	Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo
CONPES 3701 de 2011	Lineamientos de política para la Ciberseguridad y Ciberdefensa
Decreto 2609 de 2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
Ley estatutaria 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 2364 de 2012	Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012
Norma técnica colombiana NTC-ISO/IEC 27001:20013	Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
Decreto 886 de 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012. Registro Nacional de Bases de Datos.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
CONPES 3854 de 2016	Política Nacional de Seguridad digital.
Decreto 1413 de 2017	Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015 estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Resolución 0002710 de 2017 de Mintic	Por la cual se establecen lineamientos para la adopción del protocolo IPv6.
Documento CONPES 3920 de 2018	Política Nacional de explotación de datos (Big Data)
Decreto 1008 de 2018	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

Norma	Objeto
	la Información y las Comunicaciones.
Conpes 3995 de 2020	Política Nacional de Confianza y Seguridad Digital

7. Definiciones

- **Activo:** Cualquier objeto físico o intangible que tiene valor para la entidad.

- **Activo de Información:** Cualquier información o elemento relacionado con el tratamiento de esta (software, hardware, personas, etc) que tenga valor para la organización.

- **Ciberseguridad:** Conjunto de buenas prácticas para la gestión segura de la información a través de Internet.

- **Ciberdefensa:** Conjunto de políticas, acciones y buenas prácticas de orden gubernamental, en especial del gobierno nacional, para garantizar un acceso seguro al ciberespacio por parte de los ciudadanos.

- **Confidencialidad:** Atributo de la Seguridad de la Información que establece que la información solo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

- **Disponibilidad**: Atributo de la Seguridad de la Información que garantiza que la información esté disponible oportunamente y bajo los medios y formas establecidas para ser usada por las personas autorizadas.

- **Evaluación de riesgos de Seguridad de Información:** Proceso de identificación, análisis y estimación de riesgos asociados a la Seguridad de la Información.

- **Id de usuario:** En el contexto de Lotería de Medellin consiste en el elemento lógico que junto con una contraseña son requeridos para el acceso a los aplicativos, la red, correo electrónico, etc.

- **Incidente de Seguridad de la Información:** Evento o serie de eventos de seguridad de la información sorpresivos y no deseados que tienen una determinada probabilidad de comprometer las operaciones de la Entidad y amenazar la seguridad de la información.

- **Informática forense**: La informática forense, también llamada computación forense, análisis forense digital o examinación forense digital, consiste en la aplicación de técnicas científicas y analíticas especializadas que permitan identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

- **Información pública clasificada**: Es aquella información que estando en poder o custodia de la entidad, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 del 2014.

- **Información pública reservada:** Es aquella información que estando en poder o custodia de la entidad, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en la ley 712 de 2014.

- **Integridad**: Atributo de la seguridad de la información que busca mantener los datos libres de modificaciones no autorizadas.

- **IPV6:** Es el protocolo de Internet versión 6, diseñado para reemplazar la versión 4. Desde 2016 se viene implementando en la mayoría de dispositivos que acceden a Internet.

- **ISO 27001:** Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). La segunda edición fue publicada en 2013. Es la principal norma sobre la que se basa el Modelo de Seguridad y Privacidad de la Información (MSPI).

- **ISO 27002**: Código de buenas prácticas en gestión de la seguridad de la información. Primera publicación en 2005; segunda edición en 2013. No es certificable.

- **No repudio**: El no repudio o irrenunciabilidad permite probar la participación de las partes en una comunicación. Previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

- **Mabe:** Nombre del servicio de Mesa de Ayuda de la Oficina de las TIC de Lotería de Medellín**.**

- **Modelo de Seguridad y Privacidad de la Información:** Modelo formulado por el Ministerio de las Tecnologías y Comunicaciones con base en el estándar ISO 27001 y la Ley 1581 de 2012. Este modelo hace parte del programa Gobierno Digital.

- **Mspi**. Abreviatura del Modelo de Seguridad y Privacidad de la Información formulado por el gobierno nacional.

- **Plan de continuidad del negocio (Bussines Continuity Plan)**: Plan logístico orientado a garantizar que las operaciones y actividades de la entidad continúen sin interrupción en el caso de presentarse un evento o secuencia de eventos imprevistos que las ponga en peligro.

- **Política de seguridad**: Documento que contiene el compromiso de la Gerencia y el enfoque de la entidad en la gestión de la seguridad de la información.

- **Política de escritorio limpio**: Lineamientos orientados a garantizar que los usuarios mantengan su espacio de trabajo libre de cualquier tipo de información suceptible de mal uso en su ausencia.

- **Programas utilitarios.** Un programa o software utilitario, también denominado utilidad, es una aplicación de software que realiza una función determinada generalmente relacionada con la administración del sistema operativo. Como ejemplos tenemos un depurador de código, un editor, o un programa que recupera datos perdidos o borrados accidentalmente en el disco duro.

Una utilidad es una herramienta que puede realizar tareas tales como:

- Cifrado y descifrado de archivos
- Compresión de archivos
- Defragmentadores de disco
- Editores de texto
- Respaldo
- Eliminación de software maliciosos etc
- Recuperación de datos perdidos
- Tareas de mantenimiento
  Revisión de software

- **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Seguridad de la información:** Conjunto de políticas, procedimientos y prácticas orientadas a la Preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Seguridad Informática:** Aplicación de controles mediante la tecnología para la preservación de la confidencialidad, integridad y disponibilidad de la información.

- **SGSI Sistema de Gestión de la Seguridad de la Información**: Es un conjunto de políticas, procesos, procedimientos y controles para gestionar de una manera segura la información de la entidad.

- **SI:** Abreviatura de Seguridad de la Información.

- **Sistema de prevención de intrusos**: Software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

- **Software malicioso (malware):** El malware (del inglés malicious software) es cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

- **TI**: Abreviatura de Tecnologías de la Información.

- **TIC:** Abreviatura de Tecnologías de la Información y las Comunicaciones.

- **Trazabilidad**: Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.

- **Virus:** Un virus es un software que tiene por objetivo de alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario principalmente para lograr fines maliciosos sobre el dispositivo. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con

el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo producen molestias o imprevistos.

- **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

8. Vigencia

El manual de Políticas de Seguridad de la Información entrará en vigencia desde el momento en que sea aprobado por la Gerencia y/o el Comité de Gestión Institucional, y sus contenidos estarán vigentes hasta que sean suprimidos o modificados.

9. Revisión de la política

La revisión de la Política de Seguridad de la Información, se hará anualmente o cuando haya una incidencia de seguridad, evento o cambio tecnológico que amerite su revisión.

10. Política general de seguridad de la información

Lotería de Medellín ha establecido las siguientes Políticas Generales de Seguridad de la Información, las cuales representan la visión de la Entidad en cuanto a la protección de sus activos de Información:

1. Lotería de Medellín definirá e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la pérdida de integridad y garantizar la disponibilidad requerida.

2. Todos los funcionarios y/o contratistas serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

3. Únicamente se permitirá el uso de software autorizado que haya sido adquirido legalmente por la Entidad.

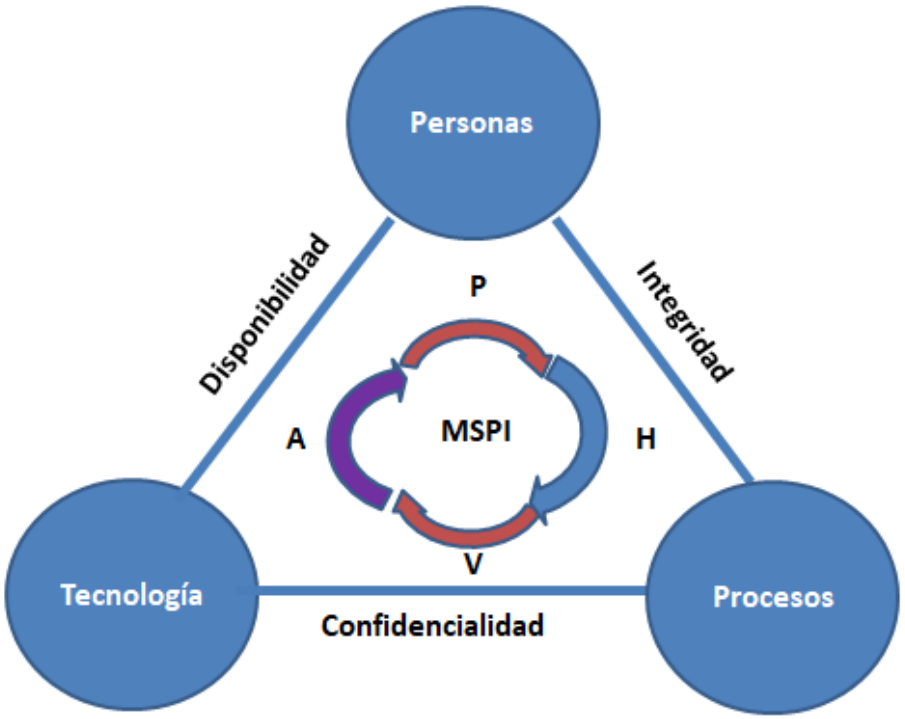
4. Es responsabilidad de todos los funcionarios y contratistas de Lotería de Medellín reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.

Lotería de Medellín contará con la documentación de los siguientes procedimientos, para asegurar la continuidad del negocio y sus operaciones ante la ocurrencia de eventos no previstos o desastres naturales.

Estos procedimientos deben contar con pruebas anuales de los sistemas más críticos y hacer las mediciones necesarias para calificar la operación y su efectividad, realizar seguimiento y generar ajustes o cambios pertinentes, estableciendo niveles de cumplimiento y protección de la información.

- ✓ Plan de Recuperación de Desastres.
- ✓ Plan de Continuidad de TI.
- ✓ Política de tratamiento de datos personales.

Adicionalmente, se establecerán las siguientes Políticas Específicas de Seguridad de la Información, las cuales se fundamentan en los objetivos de control y controles de referencia del Anexo A de la Norma Internacional ISO 27001:2013 y que hacen parte del Modelo de Seguridad y Privacidad de la Información.



Componentes de la seguridad de la información. Elaboración propia basada en https://www.owasp.org/images/9/93/Desarrollo_Seguro_Principios_y_Buenas_Pr%C3%A1cticas..pdf

A continuación se establecen 13 principios que soportan el Modelo de Seguridad y Privacidad de Lotería de Medellín:

Las responsabilidades frente a la seguridad y privacidad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, practicantes, proveedores y afiliados.

- Lotería de Medellín se compromete con el cumplimiento de la normatividad colombiana sobre protección de datos personales, en especial los lineamientos expuestos en la Ley 1581 de 2012, la Ley 1712 de 2014 y sus respectivos decretos reglamentarios.

- Lotería de Medellín protegerá la información generada procesada o resguardada por los procesos de negocio su infraestructura tecnológica, y activos del riesgo que se genera de los accesos otorgados a terceros, o como resultado de un servicio en outsourcing o tercerización.

- Lotería de Medellín protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- Lotería de Medellín protegerá su información de las amenazas originadas por parte del personal.

- Lotería de Medellín protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- Lotería de Medellín controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Lotería de Medellín implementará control de acceso a la información, sistemas y recursos de red.
- Lotería de Medellín garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- Lotería de Medellín garantizará, a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información, una mejora efectiva de su modelo de seguridad.

- Lotería de Medellín garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- Lotería de Medellín garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

11. Políticas específicas

11.1. Políticas de seguridad de la información

11.1.1. Documento de la política de seguridad y privacidad de la Información

El Manual de Políticas de Seguridad de la Información incluye las siguientes características:

- ✓ Se exponen los objetivos del MSPI y del documento.
- ✓ Se exponer el alcance de las políticas descritas en el documento.
- ✓ Las políticas de SI deben estar alineadas con los objetivos estratégicos de la entidad.
- ✓ Las políticas serán aprobadas por la gerencia y/o el Comité de Gestión Institucional.
- ✓ Las políticas deben ser socializadas permanentemente con el objetivo de que tanto los usuarios informáticos internos como externos las conozcan y las pongan en práctica.
- ✓ El documento debe contener una descripción clara del significado de Seguridad de la Información.
- ✓ Se deben definir roles, responsabilidades y responsables en la construcción y gestión del MSPI.
- ✓ Se deben definir los procesos y mecanismos para el manejo de situaciones y eventos excepcionales.

11.1.2. Revisión y evaluación

La revisión de la Política de Seguridad de la Información, se hará anualmente o cuando haya una incidencia de seguridad, evento o cambio tecnológico que amerite su revisión.

11.2. Organización de la seguridad de la información

11.2.1. Roles y responsabilidades para la seguridad de la información

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de Lotería de Medellín, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

La Gerencia y/o el Comité de Gestión Institucional de Lotería de Medellín deberá aprobar estas Políticas y será responsable de autorizar las modificaciones que se consideren pertinentes.

La coordinación de la implementación del MSPI está a cargo de la Oficina de las TIC.

11.2.2. Separación de deberes y tareas

Tanto en las responsabilidades relacionadas con la gestión de la seguridad de la información, como en los roles en los aplicativos y sistemas informáticos, se debe procurar la separación de deberes y responsabilidades, buscando que las operaciones críticas no sean ejecutadas de una sola persona.

11.2.3. Contacto con las autoridades

Se debe contar con un procedimiento y responsabilidades definidas para la denuncia de potenciales violaciones a la SI, tanto si se trata de ciber ataques (internos o externos), como la violación de la confidencialidad, integridad o disponibilidad de la información por parte de miembros de la entidad, o de cualquier otro incidente que pueda afectar la información o la plataforma tecnológica de la entidad.

11.2.4. Contacto con grupos de interés especiales

La Oficina de las TIC debe procurar mantener actualizado el conocimiento y las experticias en las temáticas relacionadas con la SI, lo que implica disponer de membresías y/o inscripciones en foros, revistas, boletines, cursos y demás fuentes de información de carácter internacional que faciliten la mejora continua en estas temáticas.

11.2.5. Seguridad de la información en la gestión de proyectos

Todos los proyectos que emprenda la entidad deben contar con una evaluación de riesgos en SI. Para esto se debe incluir en la metodología de proyectos la metología para abordar ese análisis.

11.2.6. Política para dispositivos móviles

Lotería de Medellín proveerá las condiciones para el manejo de los dispositivos móviles de la Entidad (teléfonos celulares, tabletas, entre otros), y velará porque los funcionarios hagan un uso responsable de los servicios y los equipos proporcionados.

Normas para el manejo de dispositivos móviles:

- Los funcionarios deben evitar usar los dispositivos móviles de la Entidad en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.

- Los funcionarios no deben modificar las configuraciones de los dispositivos móviles, ni instalar o desinstalar el software provisto con ellos al momento de su entrega.

- Cada vez que el sistema operativo de los dispositivos móviles notifique de una actualización disponible, deben aceptar y aplicar la nueva versión o contactar al personal de la Oficina de las TIC.
- Los funcionarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles asignados por la Entidad.

11.2.7. Teletrabajo

En necesario contar con la descripción de requisitos, mecanismos y procedimientos para el trabajo por fuera de las instalaciones de la entidad que incorporen las medidas de precaución por parte de los usuarios, así como las características de los equipos y conectividad.

La Oficina de las TIC deberá contar con una bitácora actualizada permanentemente de los empleados que laboran ocasional o permanentemente por fuera de las sedes de la entidad. Esta bitácora deberá incluir la información del equipo de cómputo, el software instalado en este, la configuración del equipo y los servicios e información a los que accede.

Las personas que laboran remotamente en forma ocasional o permanente y requieren acceder a la red corporativa de la entidad, se deben conectar a través de VPN.

Para el acceso remoto se deberá contar con el visto bueno del respectivo jefe y se deberá gestionar una solicitud a la Mesa de Ayuda.

11.3. Seguridad de los Recursos Humanos

11.3.1. Selección e investigación de antecedentes

La Dirección de Talento Humano debe realizar todas las verificaciones de los antecedentes penales y disciplinarios de los candidatos que se postulan a un cargo en la Lotería de Medellín. Estas verificaciones se llevan a cabo de acuerdo a la Ley y teniendo en cuenta la criticidad de la información a la que el candidato tendrá acceso por razones de su ejercicio laboral.

11.3.2. Términos y condiciones del empleo

El contrato de trabajo de los funcionarios de Lotería de Medellín contiene una cláusula en donde se determinan las normas esenciales para el acceso a los sistemas de información, el uso de claves, la propiedad de la información en los sistemas de información, la propiedad de los desarrollos y mejoras intelectuales realizados durante la ejecución de dicho contrato.

Los acuerdos contractuales o de confidencialidad definidos por la Entidad, reflejan los compromisos de protección y buen uso de la información y sus responsabilidades en cuanto a la seguridad de la información.

11.3.3. Responsabilidades de la dirección

Todos los directivos de la entidad deberán procurar el cumplimiento por parte de todos los miembros de la entidad de los lineamientos y normas de seguridad de la información**.**

11.3.4. Toma de conciencia, educación y formación en la SI

Todos los empleados de Lotería de Medellín y contratistas recibirán una adecuada capacitación y actualización periódica en materia de las políticas, normas y procedimientos en SI. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, en especial los asociados al manejo de contraseña segura, el cuidado ante archivos adjuntos maliciosos, el uso de mecanismos de doble autenticación, entre otros que se consideren importantes.

11.3.5. Proceso disciplinario

Se seguirá el proceso disciplinario formal contemplado en las normas estatutarias y convencionales que rigen al personal de la Administración Pública Nacional, para los empleados que violen la Política, Normas y Procedimientos de Seguridad de la Entidad.

Los funcionarios que incumplan estas obligaciones pueden incurrir también en responsabilidad civil o patrimonial cuando ocasiona un daño que debe ser indemnizado y/o en responsabilidad penal cuando su conducta constituye un comportamiento considerado delito por el Código Penal y leyes especiales.

11.3.6. Terminación o cambio de responsabilidades de empleo

La Dirección de Talento Humano debe realizar el proceso de desvinculación o cambio de labores de los funcionarios, llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin, de forma ordenada, controlada y segura. En este caso, debe solicitar a la Oficina de las TIC la modificación o inhabilitación de usuarios en los sistemas de información a los que tiene acceso.

El acuerdo de confidencialidad que se firme con los empleados de la entidad deberá incluir el tiempo que durará la obligación por parte de este una vez termine la relación laboral, de acuerdo con la criticidad de la información a la que tendrá acceso y la potencial afectación en caso de violación de dicho acuerdo.

11.4. Gestión de Activos

Los activos son todos los elementos que una organización posee para el tratamiento de la información (hardware, software, recurso humano, entre otros), estos activos se proporcionan para cumplir con los propósitos del Negocio.

Toda la información sensible de la Entidad, así como los activos donde se almacena y se procesa información, deben ser asignados a un responsable, inventariados y posteriormente clasificados.

A continuación se exponen las principales directrices para desarrollar estas labores.

11.4.1. Inventario de activos

El inventario será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad anual o cuando se requiera.
Para la descripción y clasificación de los activos de información (tangible e intangible) se debe desarrollar un documento denominado Registro de Activos de Información, de acuerdo con los lineamientos establecidos en la Ley 1712 de 2014 y el Decreto 103 de 2015. Este documento, que además debe estar alineado con la normatividad sobre gestión documental, se debe revisar y si es del caso actualizar al menos 1 vez al año, o cuando se identifiquen necesidad de reflejar cambios en este. Igualmente se debe socializar a los terceros de interés previamente identificados y caracterizados.

11.4.2. Propiedad de los activos

- Los activos de información de la entidad deben tener un “propietario” o responsable asignado, el cual deberá procurar su buen uso, cuidado y preservación. En el caso de estaciones de trabajo, el responsable será el usuario a quien se le asigne dicho equipo.

- La propiedad de los datos e información no estructurada (documentos ofimáticos) que radica en los discos duros de cada estación de trabajo corresponde igualmente al respectivo usuario.

- Las diferentes dependencias de Lotería de Medellín, deben actuar como propietarias de la información física y electrónica de la Entidad, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.

- El inventario de los activos de información debe mantenerse actualizado, acogiendo las indicaciones para la clasificación de la información.

- Los recursos de procesamiento de información de la Entidad, se encuentran sujetos a auditorías y a revisiones de cumplimiento por parte del personal asignado para esta labor.

- La Oficina de las TIC es la propietaria de los activos de información correspondientes a la infraestructura tecnológica (centro de datos, redes, etc) y en consecuencia, debe asegurar su apropiada operación y administración.

- La Oficina de las TIC es la autorizada para la instalación, configuración, cambio o eliminación de componentes de la plataforma tecnológica de Lotería de Medellín.

- Los recursos tecnológicos de Lotería de Medellín, deben ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la Entidad.

- La Oficina de las TIC debe recibir los equipos de trabajo fijo y/o portátil para su reasignación o disposición final, y generar copias de seguridad de la información de los funcionarios que se retiran o cambian de labores, cuando es solicitado formalmente.

11.4.3. Uso aceptable de los activos de información.

Los funcionarios, contratistas y terceros deberán seguir las siguientes reglas para el cumplimiento del uso aceptable de la información y de los activos asociados con los servicios de procesamiento de información:

Los recursos tecnológicos de Lotería de Medellín provistos a los funcionarios y terceros, son proporcionados con el único fin de llevar a cabo las labores de la Entidad; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.

Reglas para el uso del Correo Electrónico

a. Las cuentas de correo electrónico deben ser usadas para el desempeño de las funciones asignadas dentro de Lotería de Medellín, así mismo podrán ser utilizadas para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad.

b. Los mensajes y la información contenida en los buzones de correo son propiedad de Lotería de Medellín y cada usuario como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

c. El tamaño de los buzones de correo es determinado por la Oficina de las TIC de acuerdo con las necesidades de cada usuario y disponibilidad del servicio.

d. El tamaño de los archivos adjuntos no debe superar 25 MB. De lo contrario se debe buscar otra alternativa para compartir dicha información, con el acompañamiento de la Oficina de las TIC.

e. El envío de información corporativa debe hacerse exclusivamente desde la cuenta de correo que Lotería de Medellín proporciona.

f. El envío masivo de mensajes corporativos deberá contar con la asesoría y la autorización de la Oficina de las TIC y la oficina de Comunicaciones. Estos correos deberán incluir un mensaje que le indique al destinatario como ser eliminado de la lista de distribución, además debe ser enviado a través de una cuenta de correo a nombre de una dependencia y/o servicio habilitado para tal fin.

g. La información que requiera ser enviada fuera de la Entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas proporcionadas por la Oficina de las TIC.

h. Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por Lotería de Medellín y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

i. La Entidad tiene una cuenta de correo para el envío de mensajes masivos (todoslosempleados@loteriademedellin.com.co), la oficina de Comunicaciones es la autorizada para el envío de información a esta cuenta, sólo en casos excepcionales los Directivos y la Gerencia podrán realizar esta labor. No será entonces procedente, que alguno de los empleados diligencie en el campo “Para:” a cada uno de los colaboradores para enviar correos con contenidos personales o institucionales.

j. No está permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Entidad.

- Enviar mensajes mal intencionado que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.

- Utilizar la dirección de correo electrónico de Lotería de Medellín como punto de contacto en comunidades interactivas o cualquier otro sitio que no tenga que ver con las actividades laborales.

Reglas para el uso de Internet

a. Lotería de Medellín realizará monitoreo de los tiempos de navegación y páginas visitadas por parte de los funcionarios. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la legislación nacional vigente.

b. Los usuarios son responsables de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información.

c. Los usuarios de este servicio, no pueden asumir en nombre de Lotería de Medellín, posiciones personales en encuestas de opinión, foros u otros medios similares.

d. No está permitido:

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.

- El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, MSN Messenger, Skype y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio.

- El intercambio no autorizado de información de propiedad de Lotería de Medellín, de sus clientes y/o de sus funcionarios, con terceros.

- La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

e. El uso de Internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, responsable, no abusiva y sin afectar la productividad ni la protección de la información de Lotería de Medellín.

11.4.4. Devolución de Activos.

En el momento de desvinculación, los funcionarios deben realizar la entrega de su puesto de trabajo al Director o Jefe de Oficina respectivo o a quien este delegue. Así mismo, deben

encontrarse a paz y salvo en cuanto a los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

La Dirección de Talento Humano, debe informar con previa anticipación a la Oficina de las TIC para que se reciban los recursos tecnológicos que se le asignaron al funcionario.

La información almacenada en los equipos asignados a los funcionarios es de propiedad de Lotería de Medellín, por lo tanto; los funcionarios que se desvinculan de la Entidad tienen prohibido eliminar la información que se encuentre en los equipos de cómputo. La Oficina de las TIC realizará una copia de respaldo o backup con el fin de disponer de dicha información, en caso de ser requerida.

Adicionalmente, se debe garantizar:

- Disponibilidad de toda la información que esté bajo la responsabilidad o propiedad de dicho integrante.
- Respaldo de la información de la cuenta de correo administrada por dicho integrante y de su disco duro si es necesario.
- Entrega de contraseñas si aplica.
- Borrado seguro de información garantizando que ninguna persona no autorizada pueda acceder a información crítica de la entidad.
- Transferencia de conocimiento cuando sea necesario.

11.4.5. Clasificación de información

Dando cumplimiento al artículo 20 de la Ley 1712 de 2014 “Ley de Transparencia”, se debe generar un Registro de Activos de Información y un Índice Información Clasificada y Reservada de Clasificación de la Información donde se establezcan los niveles de criticidad y sensibilidad de los activos de información de la entidad.

Normas dirigidas a la Oficina de las TIC:

- Eliminar de forma segura la información a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando ésta ya no sea vigente o cambia de usuario.
- Definir los métodos de cifrado de la información de la Entidad de acuerdo al nivel de clasificación de los activos.

Normas dirigidas a la Subgerencia Administrativa y Financiera:

- Utilizar los medios apropiados para destruir o desechar correctamente la documentación física cuando se ha cumplido su ciclo de almacenamiento, con el fin de evitar la reconstrucción de la misma, acogiéndose a procedimiento establecido para tal fin.
- Administrar el contrato de almacenamiento y resguardo de los documentos físicos del archivo histórico de la Entidad con el proveedor del servicio.

Normas dirigidas a todos los usuarios:

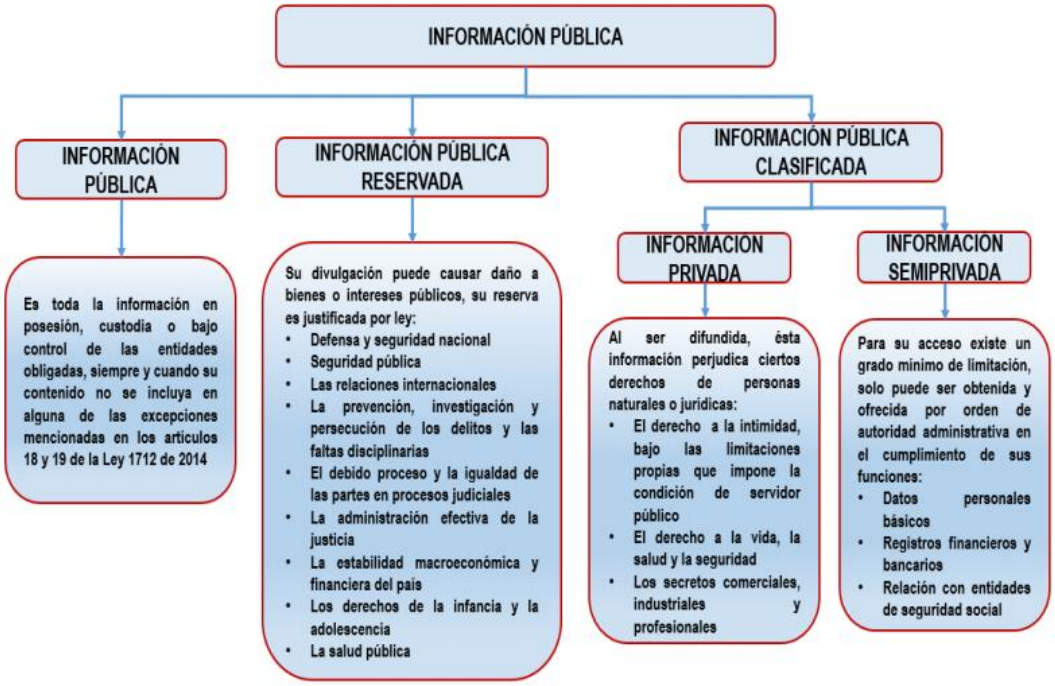
- Acatar los lineamientos de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la Entidad.

- La información física y digital de Lotería de Medellín debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.

- Cuando se impriman, escaneen, saquen copias y envían faxes, se deben verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos, además recoger inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.

- En el momento en que los funcionarios se ausenten de sus puestos de trabajo, sus escritorios deben quedar libres de documentos y medios de almacenamiento utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

- La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.



Cada activo de información debe ser clasificado de acuerdo a cada uno de los tres aspectos o aristas principales de la seguridad de la información:

Clasificación por Confidencialidad

INFORMACION PUBLICA 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.
INFORMACION PUBCLCA 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.
INFORMACION 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.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

Clasificación por Integridad

A (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
M (MEDIA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
B (BAJA)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

Clasificación por disponibilidad

1 (ALTA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
2 (MEDIA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
3 (BAJA)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

11.4.6. Etiquetado o rotulado de Activos.

Se definirán procedimientos para el rotulado y manejo de información, de acuerdo al esquema de clasificación adoptado por la Entidad. Estos procedimientos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las actividades de procesamiento de la información, almacenamiento y transmisión.

En el caso de activos tangibles, tales como equipos de cómputo, impresoras, dispositivos móviles, dispositivos extraíbles, etc, se deberá realizar un etiquetado de tal manera que se identifique inequívocamente cada uno de estos. En el caso de que estos pertenezcan a algún proveedor, se deberá exigir esta actividad en el contrato respectivo y este debe ser realizado de acuerdo con las políticas de Lotería de Medellín.

11.4.7. Manejo de activos.

Lotería de Medellín proveerá las condiciones de manejo de los tokens de seguridad para los procesos que los utilizan y velará porque los funcionarios hagan un uso responsable de estos.

Normas para el manejo de los tokens de seguridad:

- Los tokens deben ser entregados a los funcionarios designados para su uso, formalizando la entrega por medio de acta.
- Estos dispositivos son de uso exclusivo, personal e intransferible, al igual que la cuenta de usuario y la contraseña de acceso.
- El almacenamiento de estos dispositivos, debe efectuarse bajo estrictas medidas de seguridad, dentro de caja fuerte o escritorios con llave, de tal forma que se mantengan fuera del alcance de terceros no autorizados.
- Los Administradores de los tokens deben dar aviso a las entidades emisoras en caso de robo o pérdida, con el fin de efectuar el bloqueo respectivo y la reposición de los mismos.
- Los Administradores de los tokens deben realizar el cambio de estos, cuando se presente mal funcionamiento, caducidad, cambio de funciones o cambio del titular, reportando a la entidad emisora y devolviendo los dispositivos asignados.
- Los usuarios deben devolver el token asignado en estado operativo al Administrador de los tokens cuando el vínculo laboral con Lotería de Medellín se dé por terminado o cuando haya cambio de cargo, para obtener el paz y salvo, el cual será requerido para legalizar la finalización del vínculo con la Entidad.
- Los usuarios deben responder por las transacciones electrónicas que se efectúen con la cuenta de usuario, clave y el token asignado en el desarrollo de sus actividades como funcionarios de Lotería de Medellín. En caso de que suceda algún evento irregular con los tokens, los usuarios deben asumir la responsabilidad administrativa, disciplinaria y económica.

- Los usuarios no deben abrir los tokens, retirar la batería o placa de circuitos, ya que ocasionará su mal funcionamiento.

- Los usuarios no deben usar los tokens fuera de las instalaciones de la Entidad, para evitar pérdida o robo de estos.

Protección de acuerdo con la clasificación. De acuerdo con el nivel de clasificación de cada activo, se deben establecer los mecanismos de protección respectivos y de entrega formal de estos para su respectivo uso.

Adicionalmente, en el caso de la información, se debe establecer los mecanismos de protección de aquella contenida en las copias de respaldo, de tal manera que esté acorde con el nivel de protección de la información original.

Manejo de medios magnéticos. Los medios magnéticos deben estar debidamente marcados y deben ser protegidos tanto al almacenarse como al transportarse.
De otra parte, se debe garantizar que el almacenamiento del hardware (si aplica) se realiza de acuerdo con las especificaciones de los fabricantes.

Almacenamiento de la información. Toda la información propia de la gestión de Lotería de Medellín debe residir en las bases de datos, en las carpetas de red asignadas a cada área, y/o en medios de almacenamiento externo entregado y/o respaldado por tecnología, nunca en los discos duros de las estaciones de trabajo, en cuyo caso se haría responsable al respectivo usuario en caso de presentarse pérdida o daño de información.

Calidad del dato. Con el objetivo de que la información estructurada en bases de datos generada por la entidad y por externos sea de utilidad y genere valor, la entidad deberá procurar por mantener altos niveles de calidad de esta. Esto implica el cumplimiento de los lineamientos establecidos por los 4 ámbitos del dominio de información del Marco de Referencia de la Arquitectura Empresarial para la Gestión de TI generado por el Ministerio de las TIC (planeación y gobierno, diseño, análisis y aprovechamiento, y calidad y seguridad de los componentes de información)en los que están incluidos la identificación de los productores de los datos, caracterización del ciclo de vida de los datos, y la depuración de las bases de datos de tal manera que el dato sea consistente, íntegro, sin registros duplicados, y veraz.

11.4.8. Gestión de Medios Removibles.

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de Lotería de Medellín, será reglamentado considerando las labores realizadas por los funcionarios y su necesidad de uso.

Normas de uso de periféricos y medios removibles:

- Los funcionarios no deben modificar la configuración de periféricos y medios de almacenamiento.
- Los funcionarios son responsables por la custodia de los medios de almacenamiento asignados por la Entidad.
- Los funcionarios no deben utilizar medios de almacenamiento personales en la plataforma tecnológica.
- El uso de dispositivos de almacenamiento extraíbles está restringido. De ser necesario su uso, los funcionarios deben solicitar a la Oficina de las TIC le sean habilitados los puertos del equipo para que dichos dispositivos puedan ser usados.
- Si no se requiere su conservación, el contenido de cualquier medio removible que se vaya a retirar de la entidad se debe borrar de forma que no sea recuperable.
- Para la información más crítica se debe considerar la obtención de varias copias en medios separados.

La información contenida en los equipos asignados a los funcionarios es de propiedad de Lotería de Medellín, por lo tanto la información no debe ser extraída para fines que atenten contra la confidencialidad e integridad de las actividades propias de la Entidad. La Oficina de las TIC, mediante el uso de herramientas estará encargada de monitorear la información que sea extraída de la plataforma tecnológica.

11.4.9. Disposición de los medios.

Se debe contar con un procedimiento para realizar la baja de un activo de información, teniendo en cuenta la conservación de la información allí almacenada en caso de ser necesario.

11.4.10. Transferencia de medios físicos

El transporte de medios magnéticos que contengan información de la entidad debe ser realizado por empresas especializadas en ese servicio. Debe establecerse un procedimiento que permita la plena identificación de la empresa y las características de su servicio.

En caso de que esta labor sea gestionada por un proveedor, se debe exigir el cumplimiento de estos criterios y el registro de cada uno de los transportes realizados con sus características principales (origen, destino, tipo de medio, protección aplicada, tiempo de desplazamiento, información que contiene, responsables de la entrega y la recepción, entre otros datos de relevancia).

11.5. Control de acceso

11.5.1. Política de control de acceso

La Oficina de las TIC como responsable de las redes de datos y los recursos de red de la Entidad, debe vigilar porque estos sean debidamente protegidos contra accesos no autorizados.

11.5.2. Acceso a redes y servicios en red

Normas de acceso a redes y recursos de red:

- Los equipos de cómputo que se conecten a las redes de datos de la Entidad deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

- La Oficina de las TIC debe asegurar que las redes inalámbricas de la Entidad cuenten con métodos de autenticación que evite accesos no autorizados.

- Las redes de datos y los recursos de red deben estar debidamente protegidos, a través de mecanismos de control de acceso lógico, contra accesos no autorizados.

- Solo se debe permitir acceso de los usuarios a los servicios de red para los que hayan sido autorizados específicamente.
- Para la autorización de acceso a la información se debe contemplar un análisis previo de la justificación de la necesidad de uso de la misma y las actividades a realizar con el acceso a la información.

Está prohibido en las redes y servicios de red:

- Instalar o conectar sus portátiles o dispositivos personales a la red de Lotería de Medellín para realizar labores no institucionales.

- Introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.

- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.

- Albergar datos de carácter personal en las unidades de red y en las unidades locales de disco de los computadores de trabajo.

Administración remota. Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información. Todo uso de aplicaciones de conexión remota por parte de los integrantes de Lotería de Medellín deberá ser previamente solicitado por el respectivo jefe inmediato a la Mesa de Ayuda. Oficina de las TIC, por medio de la Coordinación de Infraestructura, deberá tener el control y seguimiento al uso de dichos aplicativos.

Conexiones VPN. Una conexión VPN, o Virtual Prívate Network es un mecanismo usado para conectar remotamente (vía Internet) una máquina o estación de trabajo con una red local. En el caso de Lotería de Medellín, las VPN son configuradas en las máquinas usadas por los usuarios que requieren dicha conexión.
Para proceder a su configuración se requiere previa solicitud del jefe inmediato y la aprobación por parte del Área de Tecnología e Información.

La máquina a configurar deberá ser de propiedad de Lotería de Medellín o del proveedor del servicio de arrendamiento de hardware. La máquina deberá tener contar con el software debidamente licenciado y con un antivirus actualizado.

Cuando se tenga la conexión activa, la máquina solo deberá ser usada estrictamente para los fines o propósitos establecidos en la solicitud de configuración de la VPN y evitar conectarse físicamente a otras redes locales.

La contraseña usada para la autenticación en la VPN deberá tener al menos 8 caracteres y estar compuesta por una combinación de mayúsculas, minúsculas, números y caracteres especiales.

El usuario debe recibir los lineamientos básicos para establecer la conexión VPN, y sobre las precauciones de manejo del equipo y la seguridad de la información a la que tenga acceso durante la conexión.

La Oficina de las TIC deberá mantener inventariadas y caracterizadas las estaciones de trabajo que tengan configuradas VPN, los usuarios respectivos, las carpetas a las que tiene acceso remotamente, objetivos de la conexión, fecha de instalación y demás información relevante.

Carpetas de red. Cada dependencia de la entidad cuenta con su carpeta en la red y a sus miembros se les otorga acceso y permisos de edición, de tal manera que estos tienen la posibilidad de crear, modificar y eliminar subcarpetas y documentos que se almacenen dentro de estas.

De manera excepcional, por solicitud de un jefe de área, se podrá entregar acceso (selectivamente de solo lectura o lectura-escritura) a otras carpetas a un miembro interno de la entidad.

Igualmente, de forma excepcional, se pueden generar accesos de solo lectura a proveedores o terceros (por ejemplo vía FTP) a carpetas de la red, previa solicitud de un jefe de área y de la respectiva autorización por parte del (la) jefe de Tecnología e Información.

La Oficina de las TIC deberá mantener actualizada una bitácora en la que se mapee la totalidad de las carpetas de la red, los usuarios a los que se les concede acceso, el tipo de acceso (lectura o escritura) y los cambios generados en el tiempo.

11.5.3. Registro y cancelación de usuarios.

Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de la Lotería de Medellín y se usarán exclusivamente para actividades relacionadas con la labor asignada.

El ID de usuario (loguin) en cada uno de los aplicativos y las redes informáticas de la entidad debe ser único y deben seguir la nomenclatura estandarizada para cada aplicativo.

Los integrantes con acceso a un sistema de información o a la red, dispondrán de una única cuenta de acceso compuesta de identificador de usuario y contraseña definida de acuerdo a los lineamientos de estas.

Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.

La Oficina de las TIC cancelará la cuenta o la desconectará temporal o permanentemente cuando se detecte un uso no aceptable de usuarios de acceso a la red de acuerdo con las políticas aquí establecidas. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

Los integrantes de Lotería de Medellín deben evitar intentar sobrepasar los controles de los sistemas, examinar los computadores y redes de la entidad en busca de archivos de otros sin su autorización o introducir intencionalmente software diseñado para causar daño o impedir el normal funcionamiento de los sistemas.

Las actividades asociadas a las cuentas de usuario, deben estar antecedidas de una solicitud del Jefe de Área respectivo (en el caso de colaboradores internos de Lotería de Medellín) o del propietario de la cuenta (cuando se trate de cuentas de proceso de G Suite). La solicitud debe incluir como mínimo el nombre y cédula del propietario, y en el caso de cuentas del aplicativo misional se debe agregar el rol que deberá tener. Cuando se trate de la creación de una cuenta en el ERP Sicof, se deberá contar con la aprobación del(a) Subgerente Financiero.

En caso de retiro definitivo de un empleado, sus credenciales de acceso a los sistemas informáticos de la entidad deberán ser bloqueadas en un lapso no superior a 24 horas de haberse efectuado el mismo. Para esto, el jefe inmediato deberá notificar el suceso a la Mesa de Ayuda de TI el mismo día de retiro

Igualmente las credenciales de acceso a la totalidad de los sistemas informáticos de la entidad por parte de los empleados deberán ser bloqueados durante el tiempo del disfrute de las vacaciones respectivas. Para esto, la Dirección de Talento Humano deberá compartir mensualmente a la Mesa de Ayuda de TI la programación de vacaciones del personal

En el caso de licencias, permisos e incapacidades de un empleado superiores a 10 días, las respectivas credenciales de acceso a la totalidad de los sistemas informáticos de la entidad deberán también ser bloqueadas. Para esto el jefe inmediato será quien notifique a la Mesa de Ayuda de TI la respectiva novedad a más tardar el día de inicio de la misma e indicar la fecha de finalización, en caso de prorroga esta debe ser notificada igualmente.

11.5.4. Suministro de acceso de usuarios

Lotería de Medellín establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la Entidad. Así mismo, velará porque los funcionarios tengan acceso únicamente a la información necesaria para el desarrollo de sus labores.

Normas de administración de acceso de usuarios:

La Oficina de las TIC tiene establecidos procedimientos para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la Entidad, contemplando la creación, modificación, bloqueo o eliminación de las cuentas de usuario.

Los propietarios de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

Normas de control de acceso a sistemas y aplicativos:

- Autorizar los accesos a los sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso.

- Monitorear periódicamente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

- La Oficina de las TIC tiene establecidos ambientes separados a nivel físico y lógico para desarrollo, pruebas y producción, evitando que las actividades de desarrollo y pruebas pongan en riesgo la integridad de la información de producción.

- Todos los recursos de información críticos de Lotería de Medellín tienen asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada funcionario requiere para el desarrollo de sus funciones.

- Se tienen definidos criterios para las contraseñas del directorio activo donde se registran los usuarios, estos criterios son: las contraseñas deben ser aleatorias, alfanuméricas, de ocho caracteres como mínimo y deben incluir al menos un carácter numérico y un símbolo especial, deben ser cambiadas obligatoriamente cada 65 días, tienen bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso.

- Las claves de administrador de toda la plataforma tecnológica, deben estar debidamente custodiadas en caja fuerte o lugar de acceso restringido y debe guardarse en sobre cerrado, para uso exclusivo del Jefe de la Oficina de las TIC en el evento que se requiera.

Los integrantes de Lotería de Medellín tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por la Oficina de las TIC y la autorización de su jefe inmediato.

Todas las actividades de Administración en los aplicativos deben siempre seguir los lineamientos de la Oficina de las TIC de la entidad, la cual será la responsable de configurar el rol que se le asigne a cada uno de los Administradores de los diferentes aplicativos.

La caracterización y configuración de roles en los aplicativos se deberá hacer bajo solicitud de un directivo responsable del proceso asociado al rol solicitado. Se debe evitar la duplicación de roles.

En el caso del aplicativo misional, los permisos de acceso serán establecidos de acuerdo con la configuración previa de los roles. Esta configuración, en la cual se determinan los permisos y elementos del menú al que tendrá acceso, se debe realizar en conjunto con los usuarios y la aprobación del respectivo jefe inmediato, identificando necesidades y potenciales conflictos, y teniendo siempre en cuenta los impactos que generan dichos permisos. La configuración de un nuevo rol deberá hacerse por solicitud expresa del jefe del área y/o usuario interesado. La asignación de un rol a un usuario, así como su nivel de autorización, para el caso de usuarios que deberán autorizar servicios médicos y/o medicamentos, se deberá realizar previa solicitud y/o autorización del jefe de área.

La filosofía expresada en el ítem anterior se aplica igualmente para el acceso al ERP Sicof, con la excepción de los niveles de autorización que son un concepto exclusivo del aplicativo misional.

Toda la información asociada a los usuarios delos aplicativos misionales, del ERP Sicof y la plataforma G Suite deberá ser permanentemente actualizada, revisada, y depurada si es del caso, al menos cada 3 meses con el fin de garantizar que hayan sido inactivadas o eliminadas las cuentas de usuarios retirados, que los usuarios autorizadores tengan el nivel de autorización adecuado (en el caso del aplicativo misional) y que la nomenclatura corresponda a los estándares establecidos para cada aplicativo. Cada revisión debe registrarse en un acta.

11.5.5. Gestión de derechos de acceso privilegiado

Los derechos de acceso privilegiado deben estar reservados exclusivamente para usuarios administradores de los sistemas informáticos de la entidad. Los privilegios deben ser caracterizados y los derechos de acceso a estos privilegios deben ser monitoreados y revisados periódicamente por la Oficina de las TIC.

Para mantener el control de los accesos privilegiados se debe establecer un cambio frecuente de contraseñas, así como la inactivación inmediata de usuarios administradores cuando se retiran de la entidad.
Las credenciales de acceso a las consolas administrativas con roles súper-administradores deben ser custodiadas en un sobre sellado guardado en un área segura que establezca la Oficina de las TIC, y deben ser cambiadas al menos una vez al mes.

Las contraseñas de las cuentas de usuario predefinidas correspondientes a aplicativos adquiridos deben ser desactivadas o cambiadas una vez este sea instalado.

11.5.6. Gestión de información de autenticación secreta de usuarios

Se debe contar con un proceso formal de entrega del ID de usuario y su respectiva contraseña a los miembros de la entidad, que sea ejecutado tanto en los casos de solicitud de nuevo usuario como en los de cambio de contraseña.

Mediante este procedimiento se debe resguardar la confidencialidad en el suministro de la clave a los usuarios, con la implementación de un protocolo de entrega así como el uso de mecanismos tecnológicos que garanticen su secreto. Igualmente se debe garantizar la plena identificación del destinatario antes de proceder al suministro.

La contraseña entregada es temporal y debe ser generada aleatoriamente, de tal manera que sea única. Los sistemas informáticos deben obligar al usuario al cambio de esta por una clave personal en su primer ingreso.

11.5.7. Revisión de los derechos de acceso de usuarios

Se debe contar con un procedimiento para la revisión periódica, y luego de cualquier cambio, promoción o retiro de la entidad, de los derechos de acceso de los usuarios a todos los aplicativos de la entidad, es decir, los roles, perfiles y permisos que tiene cada usuario. Esta labor debe incluir la revisión de los permisos a los usuarios privilegiados y/o administradores, haciendo énfasis en el aplicativo misional y los aplicativos de apoyo administrativo.

La Oficina de las TIC deberá mantener monitoreadas y actualizadas las matrices de roles y usuarios, o las equivalentes para cada una de los aplicativos, de tal manera que se garantice que los permisos de los usuarios satisfacen las necesidades para su desempeño laboral, basándose en el principio de mínimos privilegios.

11.5.8. Retiro o ajuste de los derechos de acceso

Ante el retiro de un miembro de la entidad, se deben inhabilitar en un lapso no superior a 24 horas las claves de acceso a todos los aplicativos que esa persona usaba.

En caso de cambio de funciones y/o de área, se deben revisar los permisos respectivos y ajustarlos a las nuevas necesidades, retirando los permisos de acceso a las funcionalidades que no requiera. El retiro o cambio de funciones del funcionario debe ser previamente informado por el Jefe de Área a través de la Mesa de Ayuda de TI.

Idéntico procedimiento se debe seguir con los permisos de acceso a los sistemas informáticos de la entidad otorgados a los usuarios externos.

11.5.9. Uso de información de autenticación secreta

Se debe contar con un procedimiento para la entrega de las claves de acceso a los usuarios, que garantice la confidencialidad de esta y que incluya los siguientes lineamientos para dichos usuarios:

- No revelar las contraseñas ya que son personales e intransferibles, por lo tanto son de carácter confidencial.

- Las contraseñas no deben estar escritas ni disponibles donde otros puedan tener acceso fácilmente a ellas.

- En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 30 días.

- Cambiar la contraseña ante cualquier sospecha de acceso indebido de esta por parte de terceros.

- Construir las contraseñas cumpliendo con los siguientes lineamientos:

  - ✓ Con 8 o más caracteres
  - ✓ Utilizar caracteres especiales (¡!$%&/+]), alfanuméricos, mayúsculas y minúsculas.
  - ✓ No repetir la contraseña anterior.
  - ✓ No usar caracteres completamente numéricos o alfabéticos idénticos consecutivos.

- La contraseña no debe ser igual a las usadas para otros aplicativos ni correos personales.

- La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos.

- En caso que el sistema no lo solicite automáticamente, se debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.

- Reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece.

- No revelar las contraseñas por vía telefónica, correo electrónico o por ningún otro medio.

11.5.10. Restricción de acceso a la información

En lo relacionado con el acceso a funcionalidades, los aplicativos misionales y de soporte usados en la entidad deben contar con las siguientes características:

- Un sistema de menú para controlar el acceso a las funciones.

- Controlar a qué datos puede tener acceso un usuario particular mediante la gestión de roles y perfiles.
- Una capa de configuración para controlar los derechos de acceso de los usuarios, (lectura, escritura, borrado y/o actualización).

- Controles de seguridad en los mecanismos de intercambio de información entre aplicaciones.

11.5.11. Procedimiento de ingreso seguro

Los sistemas informáticos usados en la entidad deben tener las siguientes características:

- En los mecanismos de ingreso de los sistemas informáticos se debe evitar los mensajes de ayuda que puedan servir de ayuda a un usuario no autorizado.
  La validación de ingreso solo debe hacerse una vez sean suministrados todos los respectivos datos.

- En caso de error al ingresar, el respectivo mensaje no debe emitir la parte que falló (usuario o contraseña).

- Los mecanismos de ingreso deben contar con protección contra ataques de fuerza bruta.

- Los sistemas informáticos deben registrar los intentos exitosos y fallidos de ingreso.

- Todo intento potencial o una violación exitosa de los controles de ingreso debe ser registrado y gestionado como un evento de seguridad.

11.5.12. Sistema de gestión de contraseñas

La funcionalidad para la gestión de las contraseñas en los sistemas informáticos debe tener las siguientes características:

- Exigir el cambio de la contraseña cuando el usuario ingresa por primera vez, suministrando una contraseña segura (mínimo 8 caracteres, compuesta por números letras mayúsculas y minúsculas y al menos 1 carácter especial).
- Disponer de una funcionalidad que permita a los usuarios recuperar y/o cambiar sus contraseñas e incluyan un mecanismo de confirmación.
- Que contenga el histórico de las contraseñas usadas por el usuario para prohibirle la reutilización de estas.
- El ocultamiento de la contraseña al momento de ingresarla.
- En lo posible, los datos de las contraseñas de los usuarios deben estar encriptados y almacenados en un repositorio diferente a los demás datos del respectivo aplicativo.
- Monitoreo permanente de la calidad de las contraseñas y los respectivos correctivos si fuese necesario.

11.5.13. Uso de programas utilitarios privilegiados

El uso, instalación, desinstalación, activación, inactivación y configuración de programas utilitarios para la administración de la plataforma tecnológica debe estar centralizada en el personal técnico de la Oficina de las TIC.

En caso de que un usuario requiera el uso de un programa utilitario específico para su labor, su jefe inmediato deberá elevar una solicitud a la Mesa de Ayuda con la respectiva justificación.

La Coordinación de Infraestructura debe tener mapeada las máquinas en las cuales están instalados y activos dichos aplicativos.

En las máquinas solo deben estar instalados los programas utilitarios estrictamente necesarios para el desempeño laboral.

Todos los anteriores lineamientos aplican para las utilidades instaladas en la nube.

11.5.14. Control de acceso a códigos fuente de programas

Las librerías y archivos de código fuente deben estar debidamente documentados con los respectivos metadatos que incluyan objeto, la fecha de la versión, número de versión, lenguaje, librerías y clases usadas, autor(es), cambios con respecto a la versión anterior, entre otros datos que se consideren de importancia.

Todo el código fuente debe estar debidamente guardado en un repositorio con acceso restringido a las personas autorizadas por el (la) Jefe de Tecnología e Información.

La entrega de librerías de código fuente a los desarrolladores (internos o externos) debe hacerse mediante un procedimiento de gestión de cambios establecido en el cual se conserve la confidencialidad de su contenido, así como el control contra copias no autorizadas y se garantice el cumplimiento de los derechos de autor.

11.6. Criptografía

11.6.1. Uso de controles criptográficos

El objetivo de la política sobre el uso de controles criptográficos es garantizar la confidencialidad, disponibilidad, integridad, autenticidad y no repudio en el manejo de información de Lotería de Medellín, de acuerdo con los niveles de clasificación y los medios utilizados para su almacenamiento, procesamiento y transmisión.

La entidad debe usar controles criptográficos para la protección de las credenciales de los usuarios de los sistemas informáticos, la de los datos sensibles (especialmente los datos personales de menores de edad y los relativos a la salud de nuestros afiliados, y para la transferencia de información crítica o sensible.

Lotería de Medellín velará porque la información de la Entidad que se encuentre dentro del índice de información clasificada o reservada, es decir, la información no pública, deberá ser cifrada, en lo posible, al momento de almacenarse y/o transmitirse por cualquier medio, bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad, siempre y cuando existe la respectiva viabilidad tecnológica y no generen lentitud y otro tipo de dificultades en cuanto a desempeño de los sistemas informáticos.
La política deberá tener en cuenta toda la información de la entidad, tanto la estructurada en bases de datos como la no estructurada (documentos electrónicos y/o escaneados, correo electrónico, entre otros), y su aplicación se hará de acuerdo con la clasificación de cada activo de información y la viabilidad tecnológica para dicha aplicación.

Para determinar los mecanismos de cifrado, se deberá tener en cuenta la normatividad colombiana vigente sobre protección de datos personales, los estándares tecnológicos de orden mundial aplicables, el análisis de riesgos en SI respectivo y la compatibilidad con la plataforma tecnológica de la entidad.

El uso de algoritmos de cifrado (simétricos y/o asimétricos) y las longitudes de clave deberían ser revisadas periódicamente para aplicar las actualizaciones necesarias en atención a la seguridad requerida y los avances en técnicas de descifrado.

11.6.2. Gestión de contraseñas de cifrado

Se debe contar con procedimientos y responsables para la administración de contraseñas de cifrado, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las contraseñas y en cuanto al reemplazo de estas.

La solicitud de la asignación de contraseñas de cifrado debe ser realizada a la Mesa de Ayuda.

Las personas a las que se les autorice el uso de contraseñas criptográficas deberán velar por la disponibilidad, integridad y confidencialidad de estas, así como por las de la información a la cual se le aplique el respectivo proceso de cifrado.

La información cifrada o descifrada deberá ser tratada de acuerdo con su nivel de clasificación y su eliminación deberá hacerse a través de un borrado seguro.

Los responsables del sistema de cifrado y de las llaves criptográficas serán las encargadas de establecer los controles para asegurar el sistema y las contraseñas, así como gestionar el acceso a los funcionarios, contratistas y terceros autorizados.

Lotería de Medellín deberá diseñar y construir los procedimientos de control y gestión para la creación, activación, distribución, recuperación y revocación de las llaves criptográficas.

Las actividades relacionadas con la administración y eliminación de las llaves criptográficas deberán ser registradas por la Oficina de las TIC.

Los funcionarios, contratistas y terceros tendrán la responsabilidad de reportar, mediante los canales autorizados, las fallas reales o potenciales y los posibles riesgos del sistema de cifrado.

Las llaves serán deshabilitadas cuando se identifique algún riesgo de divulgación, o cuando se termine la relación laboral o contractual de la entidad con los empleados, contratistas o terceros autorizados.

11.7. Seguridad física y del entorno

11.7.1. Perímetro de áreas seguras

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. Estas áreas deben estar protegidas físicamente contra accesos no autorizados, daños e interferencia.

Normas para Áreas Seguras:

- Se debe prevenir el acceso físico no autorizado, el daño y la interferencia a la información en los centros de datos y cuartos de telecomunicaciones y energía de la entidad. En los casos en que los centros de datos son de propiedad de proveedores, estos deben incluir en su certificación internacional altos niveles de protección física que garantice acceso exclusivo a personal autorizado, la protección contra eventos ambientales perjudiciales (terremotos, inundación, incendio, etc) que incluyan alarmas de monitoreo, extintores, cámaras de vigilancia para detección de intrusos, etc, y cumplir con los estándares exigidos por la norma ISO 27001 en ese sentido.

- Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por la Oficina de las TIC. Los visitantes deberán estar acompañados de un funcionario de dicha dirección durante su visita.

- La Oficina de las TIC debe registrar el ingreso de los visitantes al centro de cómputo, en una bitácora ubicada en la entrada de dicha área. El acceso a esta área solo es para personal autorizado y su ingreso se hace mediante acceso biométrico y tarjeta.

- La Oficina de las TIC debe inactivar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.

- La Oficina de las TIC debe velar porque los recursos de la plataforma tecnológica de Lotería de Medellín ubicados en el centro de cómputo, se encuentran protegidos contra fallas o interrupciones eléctricas.

- La Oficina de las TIC debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado.

- La Subgerencia Administrativa y Financiera debe velar por la efectividad de los controles de acceso físico y equipos de vigilancia implementados en la Entidad.

- Los ingresos y egresos de personal a las instalaciones de Lotería de Medellín deben ser registrados; por consiguiente, los funcionarios deben cumplir con los controles físicos implementados.

- Los funcionarios deben portar el carnet que los identifica como empleados de Lotería de Medellín en un lugar visible, en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.

11.7.2. Controles físicos de entrada

Para el acceso físico a las instalaciones de los centros de datos, de telecomunicaciones y energía deben existir controles establecidos por la Oficina de las TIC, tales como el registro con la fecha y hora de ingreso y salida de las personas, garantizar que los visitantes solo accedan a lo que está autorizado, autenticar a los visitantes, y en los casos de información crítica reforzar los controles de acceso con autenticación de doble factor.

11.7.3. Seguridad de oficinas, recintos e instalaciones

En las sedes de la entidad se deben identificar las oficinas más importantes y evaluar la criticidad de potenciales accesos no autorizados a equipos de cómputo o información relevante que se encuentren dentro de estas. En el edificio de la entidad se debe proteger con llave o tarjeta de proximidad y video-vigilancia el acceso a las oficinas de Tesorería, la Gerencia, así como los cuartos de telecomunicaciones, centro de datos y energía.

11.7.4. Protección contra amenazas externas y ambientales

Los centros de datos, de telecomunicaciones y energía, y las oficinas clave de la entidad deben estar protegidos frente a amenazas ambientales y ataques tecnológicos. Para esto se debe contar con una matriz de riesgos basada en el Anexo C de la norma 27005 que incorpore los controles correspondientes, así como la identificación de las principales vulnerabilidades y amenazas, lo que debe generar a su vez un plan de acción permanente para la mitigación de estas.

11.7.5. Trabajo en áreas seguras

Para la realización de labores dentro de los centros de datos y áreas críticas de la entidad se debe contar con un procedimiento que estandarice los protocolos necesarios tendientes a evitar acceso indebido, fuga de información, y cualquier otro riesgo que se identifique.

11.7.6. Ubicación y protección de los equipos

Lotería de Medellín para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la Entidad, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

Normas de seguridad para los equipos:

- La Oficina de las TIC debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de Lotería de Medellín.

- Los empleados y terceros que tengan acceso a los equipos que componen la infraestructura tecnológica de Lotería de Medellín no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos. Estos deben estar protegidos contra amenazas físicas y ambientales.

- La Oficina de las TIC debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la Entidad.

- La Subgerencia Administrativa y Financiera debe revisar los accesos físicos en horas no hábiles a las áreas donde se procesa información.

- La Subgerencia Administrativa y Financiera debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos de Lotería de Medellín cuente con la autorización documentada y aprobada previamente por el Jefe de Área respectiva.

- La Oficina de las TIC es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, está prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la Entidad.

- Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico, el usuario responsable debe informar a la Mesa de Ayuda en donde se atenderá, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

- Todos los usuarios deben bloquear la sesión de su estación de trabajo en el momento en que se ausenten del puesto, ésta se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

- Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

- Al finalizar la jornada laboral, es necesario salir de las aplicaciones que se estaban usando y apagar el computador.

- Los equipos de cómputo deben estar protegidos contra descargas eléctricas o picos de voltaje.

- Por ningún motivo se puede conectar en las instalaciones eléctricas soportadas por la fuente de poder ininterrumpida UPS (tomas naranjados) cualquier tipo de artefacto que no sea el computador, esto con el fin de evitar un posible corto circuito que llegue a afectar los equipos soportados en ella.

- Se deben adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética, vandalismo, entre otros.

- Todos los dispositivos que conforman la infraestructura tecnológica de Lotería de Medellín, deben contar con planes anuales de mantenimiento preventivo y se debe llevar el registro de las actividades adelantadas sobre los mismos.

- Está prohibido consumir alimentos o bebidas, fumar y portar armas al interior de centros de telecomunicaciones, energía o de procesamiento de datos.

- La instalación de cualquier tipo de software o hardware en los equipos de cómputo de Lotería de Medellín es responsabilidad de la Oficina de las TIC, y por tanto son los únicos autorizados para realizar esta labor.

- Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales, papel tapiz y protector de pantalla corporativo.

- Los empleados que requieran establecer una conexión a la infraestructura tecnológica de Lotería de Medellín a través de redes virtuales privadas (VPN), deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por la Oficina de las TIC. Las conexiones remotas distintas a VPN están totalmente prohibidas (TeamViewer, escritorio remoto de Windows, VNC y similares).

- Únicamente los funcionarios y terceros autorizados por la Oficina de las TIC pueden conectarse a la red inalámbrica de Lotería de Medellín.

11.7.7. Servicio de suministro

La infraestructura eléctrica de las sedes de la entidad, especialmente las ubicadas en el Valle de Aburra debe cumplir con la certificación RETIE. En las sedes pequeñas, en caso de no tener la dicha certificación, se debe asegurar que se cuente con energía regulada.

11.7.8. Seguridad del cableado

El cableado de energía y telecomunicaciones que transporta datos o brinda apoyo a los servicios de información debe estar protegido contra la intercepción o daño. Para tal fin se deben tener en cuenta los siguientes lineamientos:

- El cableado de energía y telecomunicaciones se debe proteger mediante canaletas.

- Los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas. Deben existir planos que describan las conexiones del cableado.

11.7.9. Mantenimiento de equipos

Los integrantes de Lotería de Medellín, salvo excepciones mencionadas adelante, deben evitar realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. El personal de la Oficina de las TIC, son los únicos autorizados para realizar la instalación y mantenimiento de cualquier tipo de software o hardware en los equipos de cómputo.

La Oficina de las TIC no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información), de manera directa o a través de terceros, a equipos que no sean usados laboralmente por personal de la entidad.

11.7.10. Retiro de activos

El retiro e ingreso de equipos de cómputo a las instalaciones de la entidad, tanto de estaciones de trabajo de la entidad como equipos personales externos debe ser registrado y monitoreado. Igualmente, se debe ilustrar permanentemente a los usuarios sobre la importancia del cuidado de la información de la entidad que reposa en los discos duros de estos.

11.7.11. Seguridad de equipos y activos fuera de las instalaciones

Con el objetivo de salvaguardar la seguridad de la información almacenada en equipos que sean retirados de las sedes de la entidad, es necesario tomar medidas de precaución, tanto por parte de los administradores de la plataforma tecnológica como de los usuarios respectivos. Se deben considerar las siguientes medidas preventivas:

- Encriptar la información, o en su defecto establecer contraseñas para el acceso a los archivos almacenados en el equipo.

- Manejar un formato de retiro y de reingreso de equipos de cómputo a la entidad de tal manera que se registre el serial o código único de numeración del equipo, el usuario responsable, la fecha y hora de retiro y el tiempo estimado de reingreso de este, acompañado de las recomendaciones de cuidado del equipo al usuario respectivo.

- Dependiendo de la criticidad de la información se debe considerar pólizas de aseguramiento que compensen los potenciales daños causados por pérdida, daño o robo de esta.

11.7.12. Disposición segura o reutilización de equipos

Cuando se decide darle de baja un equipo de cómputo o porque se trata de un equipo en arrendamiento, es necesario realizar el respectivo respaldo o backup de la información alojada en este y realizar un procedimiento de borrado seguro para garantizar que la información alojada no estará a disposición de ningún tercero.

11.7.13. Equipos desatendidos

Siempre se debe bloquear las estaciones de trabajo o terminar todas las sesiones establecidas cada vez que se retire del sitio de trabajo. Sin perjuicio de lo anterior, y transcurridos 3 minutos de inactividad, de forma automática el equipo se encontrará bloqueado, exigiendo que el empleado ingrese su usuario y contraseña para desbloquear el equipo.

En las sedes conectadas al directorio activo, el papel tapiz deberá ser cambiado de acuerdo con las fechas establecidas por la Oficina de Comunicaciones.

Se debe permitir que los usuarios de las máquinas cuyo papel tapiz no es actualizado automáticamente, puedan hacerlo manualmente en un corto lapso de tiempo. Para esto la Oficina de Comunicaciones deberá publicar el instructivo correspondiente.

11.7.14. Escritorios y pantallas limpias

Los miembros de Lotería de Medellín deben mantener su puesto de trabajo libre de documentos con información de la entidad. Estos deben siembre estar guardados en cajones o repositorios bajo llave, especialmente cuando el usuario se retira de su escritorio. La pantalla del equipo de cómputo debe ser bloqueada antes de retirarse temporalmente de su puesto de trabajo y el equipo debe ser apagado al terminar la jornada laboral.

11.8. Seguridad de las operaciones

La Oficina de las TIC, encargada de la operación y administración de los recursos tecnológicos que apoyan los procesos de Lotería de Medellín, deberá velar por mantener actualizada la documentación de los procesos operativos para la ejecución de las actividades. Así mismo, velará por la eficiencia de los controles implementados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la información manejada y asegurará que los cambios efectuados sobre los recursos tecnológicos, serán adecuadamente controlados y debidamente autorizados.

Normas de asignación de responsabilidades operativas:

- La Oficina de las TIC debe efectuar la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de la Entidad.

- La Oficina de las TIC debe contar con los manuales de configuración y operación de los sistemas operativos, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica.

- La Oficina de las TIC debe proveer los recursos necesarios para la implementación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción.

- La Oficina de las TIC debe proveer la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información de la Entidad, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.

- El profesional de riesgos debe emitir concepto y generar recomendaciones acerca de las soluciones de seguridad seleccionadas para la plataforma tecnológica de la Entidad.

11.8.1. Procedimientos de operación documentados

Los procedimientos operativos para el mantenimiento de la plataforma tecnológica deben estar documentados y al alcance de los usuarios que lo requieran. Deben incluirse al menos los siguientes procedimientos:

- Instalación y configuración de software, utilitarios, módulos, etc.
- Gestión de copias de respaldo.
- Ejecución de rutinas programadas.
- Manejo de situaciones excepcionales.
- Ruta de escalamiento para manejo, de situaciones excepcionales.
- Procedimientos de reinicio y recuperación de los aplicativos en caso de falla.
- Gestión de datos resultantes de monitoreos a los sistemas informáticos y/o logs de auditoría

11.8.2. Gestión de cambios

Todos los cambios que se realicen a la plataforma tecnológica deben realizarse considerando que tanto el software, los accesos y las versiones son adecuadamente controlados, debidamente autorizados y no disminuya los niveles de seguridad existentes.

11.8.3. Gestión de capacidad

De acuerdo con los lineamiento LI.ST.11 y LI.ST.12 del Marco de referencia de la Arquitectura Empresarial para la Gestión de TI de Mintic, se debe identificar, monitorear y controlar el nivel de consumo de los recursos críticos que son compartidos por los Servicios Tecnológicos, y administrar su disponibilidad actuando de una manera preventiva y actuando en los tiempos establecidos ante las alertas tempranas que se generen.

Basándose en la información generada por dicho monitoreo, se deben realizar los ajustes necesarios y las proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema en el tiempo.

11.8.4. Separación de los ambientes de desarrollo, pruebas y producción

Los ambientes de desarrollo, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad. Los programas que se encuentren

en el ambiente de producción, pueden ser modificados únicamente por personal autorizado. Durante la fase de pruebas se debe evitar el uso de datos sensibles. Los ambientes de pruebas y de producción deberán tener rótulos distintivos para identificarlos fácilmente.

11.8.5. Controles contra códigos maliciosos

Todos los recursos informáticos de Lotería de Medellín donde se procesa y almacena información, deben estar protegidos por herramientas y software de seguridad, para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso (virus de computador, gusanos en la red, caballos troyanos y bombas lógicas).

Normas de protección:

- La Lotería de Medellín debe proveer herramientas tales como antivirus, antimalware, anti spam y antispyware para reducir el riesgo de contagio de software, además asegurar que estas herramientas cuenten con licencias de uso requeridas, certificando su autenticidad, actualizaciones periódicas y parches de seguridad.

- La Lotería de Medellín debe velar para que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus.

- La información que se encuentra contenida y es transmitida por el servicio de correo electrónico, es analizada y escaneada por la plataforma Google, en la cual se encuentra nuestro servicio de correo corporativo.

- Los usuarios deben ejecutar el software de antivirus sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos y evitar usar medios de almacenamiento de procedencia desconocida.

- Los usuarios deben asegurarse que los archivos adjuntos, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos de la Entidad.

- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar a la Mesa de Ayuda, para que se tomen las medidas de control correspondientes.
- Los equipos que se conecten a la red de la Entidad, así sean de propiedad de terceros o contratistas, se les debe instalar el antivirus que opera actualmente, esto para su escaneo y protección de información.

- Se deben establecer procedimientos y responsabilidades en la gestión de la protección contra software malicioso, documentación de los incidentes con software malicioso, versionamiento del software de protección, entre otras tareas relevantes.

- Los usuarios deben evitar escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier computador o red de Lotería de Medellín.

- Para la protección perimetral se deben disponer de listas blancas y listas negras configuradas en los Firewall (cortafuegos).

- Se deben realizar periódicamente análisis de vulnerabilidades técnicas de las redes e implementar las recomendaciones correspondientes.

- Se deben realizar periódicamente revisiones de seguridad de los aplicativos y validar que no haya presencia de archivos maliciosos.

11.8.6. Respaldo de la información

Lotería de Medellín debe asegurar que la información contenida en la plataforma tecnológica de la Entidad, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad.

Normas de copias de respaldo de la información:

- La Oficina de las TIC realiza respaldo periódico de toda la información que reposa en el centro de datos principal de la Entidad. La información es guardada en cintas, las cuales son debidamente custodiadas por un tercero en instalaciones diferentes al Edificio de Lotería de Medellín.

- La Oficina de las TIC tiene definido el procedimiento de resguardo y recuperación de la información, el cual incluye especificaciones acerca del traslado, frecuencia, identificación de la información, la ubicación física para permitir un rápido y eficiente acceso a los medios.
- Se debe contar con una política definida de respaldo que indique el tipo de respaldo (incremental o Full), frecuencia de retención, información a respaldar y demás características necesarias.

- Se debe llevar un registro detallado de las copias de respaldo que contenga las principales características, tales como la fecha, hora, tipo de respaldo (Incremental o Full), frecuencia (diaria, semanal, mensual), tamaño, información respaldada, nombre de quien lo realizó, medio de almacenamiento, etc.

- La Oficina de las TIC debe contar con un plan de restauración de copias de seguridad que serán probados a intervalos regulares, con el fin de asegurar que sean confiables en caso de emergencia.

- Es responsabilidad de los usuarios de la plataforma tecnológica de Lotería de Medellín, identificar la información crítica a su cargo y que debe ser respaldada y almacenada de acuerdo con su nivel de clasificación.

- A petición de los Jefes de las áreas, se pueden realizar respaldos a los equipos de cómputo de los usuarios informáticos internos de la entidad.

11.8.7. Registro de eventos

Los aplicativos misionales y de apoyo administrativo deben contar con una funcionalidad de log de actividades (sin afectar el rendimiento de la aplicación), que permita registrar el usuario, fecha y hora de inicio y fin de sesión, actividades realizadas, IP de conexión, número de intentos de ingreso fallidos, alarmas disparadas en los intentos de acceso fallidos, activación o desactivación de control antivirus.

11.8.8. Protección de la información de registro

Los log de actividades de los usuarios finales deben ser guardados y respaldados en repositorios a los que solo acceda el personal autorizado. Se debe garantizar que la información de los log no sea alterada voluntariamente.

11.8.9. Registros del administrador y del operador

Los logs de actividades de los usuarios administradores deben ser guardados de manera independiente al de los usuarios finales.

11.8.10. Sincronización de relojes

Los servidores de los centros de datos deberán estar sincronizados con respecto a la hora exacta de Colombia.

11.8.11. Instalación de software en sistemas operativos

Con el objetivo de proteger la plataforma tecnológica de la entidad de los impactos del software malicioso, y garantizar el cumplimiento de la normatividad en términos de derechos de autor en licenciamiento de software, se deben tener en cuenta los siguientes lineamientos:

- La instalación y/o actualización de software en general debe ser realizada exclusivamente por personal de la Oficina de las TIC debidamente autorizado.
  Solo se debe instalar archivos ejecutables previamente revisados y aprobado por la Oficina de las TIC.

- Las aplicaciones y el software a instalar debe ser debidamente sometido a pruebas exitosas que incluyan usabilidad, la seguridad, los efectos sobre otros sistemas y la facilidad de uso.

- Se debe contar con un sistema de control para mantener mapeadas todas las configuraciones del software implementado, así como la documentación del sistema.

- Debe existir una estrategia que permita fácilmente retroceder los cambios realizados en los cambios o instalación de aplicativos.

- Es necesario mantener un log de auditoría de todas las actualizaciones de las bibliotecas de los diferentes aplicativos.

- Las versiones anteriores de los aplicativos se deben conservar como una medida de contingencia.

- Se debe contar con un repositorio para el almacenamiento y manejo documental de las versiones anteriores de los aplicativos, acompañadas de toda la información sobre parámetros, configuración, software de soporte.

11.8.12. Gestión de las vulnerabilidades técnicas

Se deben realizar periódicamente análisis de vulnerabilidades, que pueden incluir test de penetración. Esta labor debe ser realizada por terceros ajenos a la entidad con el objetivo de garantizar imparcialidad en las tareas que conlleva y en los resultados arrojados. Las características y el alcance los análisis de vulnerabilidades técnicas deberán ser determinados por la Oficina de las TIC de acuerdo con las necesidades y el presupuesto disponible, priorizando los elementos que presenten mayor riesgo.

Se debe llevar un registro pormenorizado de los hallazgos, las recomendaciones de remediación y su respectiva implementación.

Se deben establecer los responsables de llevar a cabo la gestión de todas las tareas asociadas al análisis de vulnerabilidades y su respectiva remediación.

La implementación de las recomendaciones debe estar antecedida de sus respectivas pruebas para validar que no afectan el funcionamiento correcto de los sistemas informáticos.

Se debe hacer evaluación y seguimiento periódicos de la gestión de vulnerabilidades técnicas, analizando sus impactos, con el objetivo de maximizar su eficacia y eficiencia.

11.8.13. Restricciones sobre la instalación de software

La instalación de software es una labor exclusiva de la Oficina de las TIC, y por lo tanto se debe bloquear ese permiso a los demás usuarios.

11.8.14. Controles sobre auditorías de sistemas de información

Se debe evitar que las auditorías que se realicen a los sistemas informáticos de la entidad entorpezcan o interrumpan la normal operación de estos.

Para esto se debe realizar un plan debidamente aprobado por la Oficina de las TIC en el que se defina claramente el alcance de la auditoria. En lo posible se deberá crear una imagen fiel de los datos en un ambiente diferente al de producción para realizar la auditoría. En caso de que se requiera acceso a los datos en el ambiente de producción, este deberá ser de solo lectura y en horario no laboral para no afectar el rendimiento de la plataforma.

Se debe manejar un log de auditoría que registre los usuarios, fecha y hora de ingreso y salida, y las actividades realizadas.

11.9. Seguridad de las comunicaciones

11.9.1. Controles de redes

La Oficina de las TIC debe establecer los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

Normas de gestión y aseguramiento de las redes de datos

- La plataforma tecnológica de Lotería de Medellín está separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones de redes con terceros y del servicio de acceso a Internet.

- La Oficina de las TIC como administrador de los recursos tecnológicos, es responsable de garantizar que los puertos físicos y lógicos que están permitidos, estén siendo monitoreados con el fin de prevenir accesos no autorizados.

- Los procedimientos para la gestión de las redes deben estar debidamente documentados y actualizados. La gestión de la red deberá ser gestionada exclusivamente por la Oficina de las TIC o por terceros debidamente coordinados por esta.

- *Redes locales y Wifi*. Se deben mantener y controlar adecuadamente las redes para protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones que utilizan las redes, incluyendo la información en tránsito. Se debe monitorear mediante software los tiempos de respuesta, la capacidad, latencia de red excesiva y seguimiento de la conectividad a modo de garantizar la transmisión de datos entre los terminales de manera rápida y constante de dispositivos de red, tales como canales, servidores y aplicaciones.

- Las páginas de Internet a las que se tiene acceso son las validadas y definidas por la Oficina de las TIC, basándose en las políticas laborales establecidas por la Gerencia de la entidad.

- El acceso a Internet se restringe por medio del sistema de seguridad con Firewall incorporado en la misma. La Oficina de las TIC deberá velar porque el Firewall esté siempre actualizado en cuanto a las políticas de filtro de sitios no autorizados.

- Salvo excepciones autorizadas por los respectivos jefes, el acceso a sitios de redes sociales está prohibido y su acceso debe estar bloqueado.

- No está autorizada la descarga de Internet de programas informáticos no autorizados por la Oficina de las TIC.

- La Oficina de las TIC se reserva el derecho de llevar un registro de los eventos asociados a la conexión de los diferentes usuarios para asegurar el uso apropiado de los recursos de red.

11.9.2. Seguridad de los servicios de red

Para la gestión de los servicios de red tales como DNS, FTP, DHCP, Impresión, Directorio Activo y otros, se deben tener establecidos y documentados los procedimientos y manejar los protocolos y configuraciones teniendo en cuenta los principios de la SI (confidencialidad, integridad y disponibilidad).

En el servicio de impresión se debe asegurar la operación correcta y segura. Para esto se debe tener en cuenta:

- Los documentos que se imprimen deben ser de carácter institucional.

- Las estaciones de trabajo deberán tener configurada la impresión retenida, de tal forma que luego de enviar un documento a impresora, se requiera dar la orden directamente en el panel de control de esta para la impresión. Con esto se garantiza que un documento impreso pueda ser visto solo por su dueño.
- No imprimir correos electrónicos a menos que sea estrictamente indispensable. En caso de necesitar la impresión, revisar el documento y eliminar el contenido que no se requiere.

11.9.3. Separación en las redes

Las plataformas tecnológicas que soportan los sistemas de información de Lotería de Medellín deben estar separadas en segmentos de red lógicos, independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet. La división de los segmentos lógicos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad. La segmentación deberá realizarse con criterios de criticidad de la información y de agrupación de usuarios por áreas.

11.9.4. Políticas y procedimientos de transferencia de información

El correo electrónico y el internet, como herramientas para facilitar la comunicación y la transferencia de información entre funcionarios y terceros, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que lo requieran, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de estos medios.

Se debe contar de mecanismos, incluido el de autenticación, para proteger los datos e información no estructurada que son transferidos internamente y externamente en la entidad contra copia, interceptación, eliminación, modificación y enrutado.

Cuando se considere pertinente, se deben encriptar los datos antes de ser transferidos.

Estos mecanismos deben incluir la detección y bloqueo de software malicioso.

11.9.5. Acuerdos sobre transferencia de información

Para cada relación con un tercero que implique intercambio de información por medios electrónicos se debe considerar la firma de un acuerdo que incluya:

- Descripción del procedimiento para garantizar la trazabilidad de la información intercambiada y evitar el no repudio.

- Definición de estándares técnicos mínimos (empaquetado, transmisión, identificación, etc).
- Establecer las responsabilidades, obligaciones y canales de escalamiento en el caso de incidentes de SI (pérdida o ruptura de la integridad de los datos, por ejemplo).

- Método de identificación de información sensible que requiera protección especial.

- Opcionalmente, mecanismos de encriptación.

11.9.6. Mensajería electrónica

Lotería de Medellín gestiona la mensajería electrónica a través de la suite de Google G Suite, la cual tiene incorporadas múltiples aplicaciones, entre las que se destacan el correo electrónico, el calendario, el drive, herramientas ofimáticas, entre otras.

Para la autenticación a G Suite se cuenta con una única contraseña y un usuario bajo el usuario@loteriademedellin.com.co

El servicio de correo ha sido concebido como medio formal de comunicación y es una herramienta de uso institucional, por lo tanto, debe darse un uso racional mediante el envío de comunicaciones cortas y precisas. Las comunicaciones electrónicas deben tener las características básicas de cordialidad, respeto, deben observarse los conductos regulares y seguir los siguientes lineamientos:

- Se debe proteger el servicio de correo electrónico frente a problemas que se materializan por estos medios tales como: correo no solicitado (en su expresión inglesa “spam”), programas dañinos constituidos por virus, gusanos, troyanos, espías, código móvil, entre otros.

- El correo electrónico no se debe usar para envío masivo, materiales de uso no institucional o innecesarios (entiéndase por correo masivo todo aquel que sea ajeno a la

entidad, tales como cadenas, publicidad y propaganda comercial, política, social, etcétera).

- Los integrantes de Lotería de Medellín deben evitar abrir correos con archivos adjuntos desconocidos o con mensajes sugestivos.

- No se debe utilizar el correo para realizar inscripciones en redes sociales, foros entre otros, excepto para inscripciones institucionales.

- La Oficina de las TIC por medio de la Mesa de Ayuda será la única área encargada de crear las cuentas de G Suite a los usuarios para el uso de correo electrónico. Para efecto de asignarle la cuenta al usuario, el respectivo jefe inmediato deberá informar a la Mesa de Ayuda el ingreso del funcionario a la entidad, y deberá solicitar la creación de la cuenta.

- La cuenta será activada en el momento en que el usuario ingrese por primera vez a G Suite y será obligatorio el cambio de la contraseña de acceso inicialmente asignada.

- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán deberán estar constituidas por combinación de caracteres alfabéticos, numéricos y especiales.

- La Oficina de las TIC promoverá buenas prácticas de seguridad entre los usuarios y monitoreará la seguridad de las contraseñas. Igualmente publicará tips de G Suite que faciliten su uso, lo que incluye la inscripción del número de celular, registro de cuenta de correo de recuperación, pasos para la recuperación de la contraseña, entre otros.

- El retiro de los colaboradores de la entidad deberá ser notificado a la Oficina de las TIC por el respectivo Jefe Inmediato. La Mesa de Ayuda deberá generar, en caso de ser solicitado, el respectivo respaldo, incluyendo el correo, las conversaciones de Hangout (chat) y los archivos de herramientas de oficina (hoja electrónica, procesador de texto y presentador de diapositivas) y luego proceder a la eliminación de la respectiva cuenta de G Suite.

- Cada vez que se solicita la inactivación o eliminación de una cuenta de G Suite se debe verificar si la cuenta tiene archivos compartidos con terceros, y en ese caso indagar con su propietario o responsable si estos requieren seguir teniendo acceso a dichos archivos, con el objetivo de montarle los archivos respaldados a las cuentas consumidoras antes de eliminar la cuenta en cuestión.

- Las credenciales de acceso a la Suite de Google por parte de los empleados deberán ser bloqueados durante el tiempo del disfrute de las vacaciones respectivas. Para esto, la Dirección de Talento Humano deberá compartir mensualmente a la Mesa de Ayuda de TI la programación de vacaciones del personal.

- En los grupos cuyo objetivo principal sea el de envío de mensajes a sus miembros por parte de la Oficina de Comunicaciones, el permiso de hacerlo deberá tenerlo únicamente el o los propietarios de dicho grupo. Este es el caso de grupos de las sedes, por ejemplo. En los grupos menos numerosos, por ejemplo los creados con el objetivo de comunicación entre los miembros de una coordinación, el líder del equipo podrá autorizar a todos los miembros para enviar mensajes.

- Se debe hacer un barrido y eliminación frecuente de los grupos vacíos de G Suite, es decir, aquellos que no tienen miembros. En estos grupos, aunque están activos, los mensajes que le son enviados nadie los recibe pero tampoco le rebotan al emisor, quedando la sensación para este último de que alguien recibió su mensaje.

- En lo posible se debe evitar el renombramiento de cuentas de G Suite, ya que esto exige esa misma actualización en cada uno de sus contactos. Es preferible su eliminación y la instalación del respaldo en la cuenta de quien lo requiera o previamente redireccionar los correos hacia esa nueva cuentas.

- El rol de Superadministrador de G Suite se entregará exclusivamente a los miembros de la Mesa de Ayuda o a quien determine el (la) Jefe de la Oficina de las TIC. El Superadministrador será quien otorgue permisos a los Administradores, a través de los cuales se gestionarán todas las cuentas, incluyendo la creación, inactivación y reactivación, eliminación, creación y eliminación de grupos, agregar miembros a grupos, asignar alias a una cuenta, recuperación de cuentas eliminadas, generación de informes, entre otras labores.

- En el cuerpo de los correos deberá incorporarse un mensaje alusivo a la importancia de guardar la confidencialidad de la información contenida en el respectivo mensaje.

- Todas las cuentas corporativas personales (aquellas pertenecientes al dominio loteriademedellin.com.co deberán tener asignada una firma o pie que identifique al propietario de esta. Dicha firma deberá ser gestionada por la Oficina de Comunicaciones.

- Para la asignación de las licencias ilimitadas de G Suite (Business) se deben priorizar las cuentas de los directivos y las de procesos. Las restantes (dependiendo de su

disponibilidad) se deben asignar a aquellos usuarios con licencias tipo Basic que presenten altas cuotas de almacenamiento. En casos excepcionales de alto consumo, el Coordinador de Mesa de Ayuda podrá determinar el cambio de un tipo de licencia Basic por una Business.

- La Oficina de las TIC deberá velar por mantener actualizadas las configuraciones de la plataforma de G Suite, procurando mantenerla protegida contra ataques maliciosos.

11.9.7. Acuerdos de confidencialidad o de no divulgación

Para procurar un alto nivel de confidencialidad en el manejo de la información relacionada, por una parte con datos personales, y de otra parte e información transaccional de la Entidad, Lotería de Medellín deberá firmar un acuerdo de confidencialidad en el contrato laboral o de prestación de servicios. Adicionalmente, deberá establecer los adecuados controles tecnológicos tendientes a disminuir el riesgo de la ruptura de la confidencialidad.

11.10. Adquisición, desarrollo y mantenimiento de sistemas de información

Lotería de Medellín debe asegurar que el software adquirido y desarrollado tanto al interior de la Entidad como por terceros, cumplirá con los requisitos de seguridad y calidad que apunten a la protección de la información.

Requisitos de seguridad para la Oficina de las TIC:

- Establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro.

- Propender por la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.

- Contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la Entidad.

- Asegurar que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento, el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

Lotería de Medellín debe analizar e incorporar aquellos componentes de seguridad y privacidad de la información que sean necesarios en todas las etapas del ciclo de vida de las aplicaciones y sistemas de información, de acuerdo con el lineamiento LI.SIS.22 del Marco de Referencia de la Arquitectura Empresarial generado por Mintic.

Para todos los aplicativos, incluidos en lo que aplique, los genéricos de orden mundial (sistemas operativos, gestores de bases de datos, aplicativos ofimáticos, etc), se deben tener en cuenta los siguientes lineamientos:

- La adquisición, desarrollo y/o contratación de aplicativos o sistemas de información debe estar liderada, coordinada, gestionada y exclusivamente por la Oficina de las TIC. Este proceso debe realizarse en lo posible con el acompañamiento del líder o encargado del proceso asociado a dicha aplicación.

- Se debe garantizar el cumplimiento de la normatividad en cuanto a propiedad intelectual y derechos de autor.

- La adquisición y/o desarrollo de aplicaciones, paquetes de software o módulos de uno existente en la entidad, debe estar debidamente justificada y debe siempre apuntar al mejoramiento de la productividad y seguridad de los procesos de la entidad. En consecuencia, el "propietario" o doliente a quien se le asigne este como activo de información deberá garantizar su uso, y por lo tanto, el retiro o abandono de dicho aplicativo debe obedecer a un cambio o desaparición del proceso soportado por este, o a su obsolescencia debidamente certificada por la Oficina de las TIC.

11.10.1. Análisis y especificación de requisitos de seguridad de la información

Al realizar el levantamiento de requisitos para un aplicativo se deben tener en cuenta los requisitos en SI, de tal manera que queden incluidos los siguientes aspectos:

- Definir el procedimiento para el suministro de datos de autenticación de los usuarios, tanto los usuarios finales como los privilegiados o técnicos.

- Notificar oportunamente los deberes y responsabilidades a los usuarios.
- Establecer las necesidades de protección de activos de información impactados.

- Se deben tener en cuenta los requisitos para el funcionamiento correcto de otros mecanismos de control de SI.

11.10.2. Seguridad de servicios de las aplicaciones en redes públicas

Es necesario proteger la información involucrada en los servicios de aplicaciones que pasan sobre redes públicas (en especial vía internet) de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.

Para esto se requiere:

- Definir el nivel de protección requerido para mantener la confidencialidad e integridad de la información.

- Determinar el tipo, medio y alcance del mecanismo de autenticación que se debe usar para lograr el suficiente nivel de confianza requerido en relación a la criticidad de la información que se va a exponer.

- En el caso de servicios proporcionados por terceros en los mecanismos de comunicación para los servicios de aplicaciones, es necesario asegurar que estos estén completamente informados del alcance de sus servicios.

- Evitar la pérdida o duplicación de información.

- Determinar y cumplir los requisitos para lograr la confidencialidad, la integridad y el no repudio en la prueba de envío y recepción de documentos clave.

- Definir la responsabilidad asociada con cualquier actividad fraudulenta.

- Usar mecanismos de chequeo para verificar la integridad del software, firmware, e información.

11.10.3. Protección de transacciones de los servicios de las aplicaciones

La información involucrada en las transacciones de los servicios en línea debe ser protegida para evitar su divulgación no autorizada, el enrutamiento errado, la duplicación o reproducción no autorizada de mensajes la transmisión incompleta y la alteración fraudulenta de mensajes. Para esto es preciso:

- Asegurar el uso de firmas electrónicas por cada una de las partes involucradas en la transacción.

- Validar y verificar la información de autenticación secreta de usuario.

- Asegurar que la transacción permanezca confidencial.

- Mantener la privacidad asociada con todas las partes involucradas.

- Asegurar que las comunicaciones entre todas las partes esté encriptada.
- Establecer que los protocolos usados para comunicarse entre todas las partes involucradas estén asegurados.

- Asegurar que el almacenamiento de los detalles de la transacción esté afuera de cualquier entorno accesible públicamente, esto es, que no esté accesible directamente desde Internet.

- Utilizar una autoridad confiable para emitir y mantener firmas digitales o certificados digitales.

- La seguridad está integrada e incluida en todo el proceso de gestión de certificados/firmas de un extremo a otro.

11.10.4. Política de desarrollo seguro

Se deben tener en cuenta las recomendaciones entregadas por referentes de orden mundial en seguridad del código fuente, tales como la OWASP, y realizar las pruebas respectivas.

Para las etapas de desarrollo y pruebas se deben contar con ambientes separados entre sí y diferentes al de producción, garantizando que personal externo a la entidad no tenga acceso a datos reales de la entidad.

Los mecanismos y buenas prácticas en SI deben ejecutarse en todas las etapas del ciclo de vida del desarrollo de un aplicativo y deben estar contempladas en la metodología para la construcción de sistemas informáticos.

Durante el proyecto de construcción de un aplicativo se deben identificar puntos de chequeo en los hitos establecidos.

El manejo de aplicativos de control de versiones debe incluir restricciones de acceso y mecanismos de SI.

Se debe determinar la capacidad de los desarrolladores para prevenir eventos de SI, así como para encontrar bugs o vulnerabilidades

11.10.5. Procedimientos de control de cambios en sistemas

Los procedimientos de control de cambios de los aplicativos deben incluir:

- Aprobación de los cambios antes de su aplicación o implementación.

- Garantizar que las validaciones, controles y procedimientos para conservar la integridad de los datos no se van a ver afectados con los cambios.

- Implementar un estricto control de versiones para todas las actualizaciones de los aplicativos.
- Log o registro de auditoría de todos los cambios.

- Validar que los usuarios aceptan, entienden y asimilan los cambios.

- Los cambios deben estar debidamente documentados.

- La documentación que es reemplazada se debe preservar en el archivo de la entidad y caracterizarse debidamente en el sistema de gestión documental.

- Los manuales, instructivos y demás documentación operativa de usuarios finales y/o administrativos deben ser adaptados a los cambios.

- Asegurar que la implementación de los cambios ocurre en el momento correcto y no afecta los procesos de negocio involucrados.

11.10.6. Revisión técnica de las aplicaciones después de cambios

Después de cada cambio o actualización, o puesta en marcha de nuevos módulos de un aplicativo es necesario realizar pruebas técnicas, funcionales y del código de acuerdo con un plan de pruebas debidamente aprobado por la Oficina de las TIC.

11.10.7. Restricciones en los cambios a los paquetes de software

Los cambios en los aplicativos deben tener unas motivaciones claramente establecidas y justificadas desde lo operativo. Se deben evitar cambios permanentes que no aporten valor agregado sustancial a los procesos de la entidad. Todos los cambios deben ser controlados estrictamente para no poner en riesgo la operación de la entidad.

11.10.8. Ambiente de desarrollo seguro

En todas las etapas del ciclo de vida de los sistemas de información, tanto misionales como de apoyo, se debe realizar un análisis a profundidad de los riesgos y la implementación de

los controles respectivos con el objetivo de preservar altos estándares en seguridad de la información.

11.10.9. Desarrollo contratado externamente

Lotería de Medellín establecerá mecanismos de control en sus relaciones con terceros, con el objetivo de asegurar que la información a la que tengan acceso, cumplan con las políticas, normas y procedimientos de seguridad de la información.

Normas de seguridad en la relación con terceros:

- Los funcionarios responsables de la realización y/o firma de contratos o convenios con terceros se asegurarán de la divulgación de las políticas, normas y procedimientos de seguridad de la información.

- En los estudios de conveniencia y oportunidad que se realizan en Lotería de Medellín para la contratación con terceros, se tienen definidos y clasificados los riesgos (jurídicos, financieros, técnicos) y la mitigación respectiva, para garantizar la seguridad y la integridad de los servicios.

- La Oficina de las TIC establece las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la Entidad.

Los desarrollos contratados externamente deberán realizarse usando las metodologías, estándares, librerías reusables, frameworks y lenguajes que establezca la Oficina de las TIC, conservando la compatibilidad con la plataforma de la entidad.

Cuando se trate de desarrollos contratados externamente, se debe garantizar la separación de los ambientes de desarrollo, prueba y producción, garantizando que los miembros del equipo de desarrollo solo tengan acceso a los ambientes de desarrollo y pruebas.

Las cláusulas del contrato deben garantizar el gobierno por parte de la entidad sobre el código fuente (incluido las librerías que sean desarrolladas dentro del contrato o suministradas por la entidad), las metodologías de desarrollo, los archivos ejecutables, los logs y datos de pruebas.

11.10.10. Pruebas de seguridad de sistemas

Para todo nuevo aplicativo o módulo de software se deberán realizar las respectivas pruebas funcionales de seguridad, previa a su implementación. Esto es:

- El acceso por parte de los usuarios finales y administradores a los aplicativos se deber gestionar mediante la asignación de los respectivos ID de usuario (login) y clave de acceso.

- Autenticación (logín único) cumpliendo con la nomenclatura establecida, obligatoriedad de contraseña segura, ocultamiento visual de la contraseña, recuperación de contraseña, captcha o mecanismo que evite el uso de robots de autenticación, obligatoriedad de cambio de contraseña cada mes.

- Los aplicativos deben tener configurados un conjunto de roles y/o perfiles (de acuerdo con su arquitectura), que serán asignados a cada usuario de acuerdo con lo autorizado por cada uno de los jefes inmediatos, previo acompañamiento por parte de la Oficina de las TIC teniendo en cuenta las matrices de riesgos y compatibilidades de roles.

- Funcionamiento del aplicativo en las más recientes versiones de los navegadores comercialmente más usados (Microsoft Edge, Mozilla Firefox, Google Chrome y Opera).

- Mecanismo para recuperación de contraseña.

- Control de acceso exclusivamente a los módulos del menú asignados al rol respectivo.

- Niveles de acceso (lectura, modificación, agregar registros, eliminación) de acuerdo con los permisos establecidos para el rol.

- Test de penetración de acuerdo con las características del aplicativo

11.10.11. Prueba de aceptación de sistemas

Tanto los aplicativos nuevos como los cambios o mejoras hechas a estos deben ser aceptados por los respectivos usuarios. Para esto deben realizarse unas pruebas de aceptación, y acordarse previamente con estos unos criterios de aceptación, de tal manera que no haya diferencias entre las partes de cuando se dan por aceptados los componentes del nuevo desarrollo.

11.10.12. Protección de datos de prueba

Para el acceso a los datos de prueba se debe contar con los mismos mecanismos e iguales restricciones que se tienen para los datos en producción.

Cada vez que se vaya a realizar copia de datos de producción en el ambiente de pruebas, es necesario contar con la debida autorización de la Oficina de las TIC.

Se debe generar un log de auditoría cada vez que se realicen copias del ambiente de producción al de pruebas. Una vez finalice cada sesión de pruebas, los respectivos datos deben ser eliminados de una manera segura.

11.11. Relación con proveedores

11.11.1. SI en las relaciones con los proveedores

Para cada uno de los contratos que la entidad firme con proveedores, se debe identificar la información que se va a intercambiar con este y/o a la que va a tener acceso y/o la que va a ser producida por dicho proveedor.

Se debe evaluar la criticidad de la información teniendo en cuenta los procedimientos para su clasificación y se deben prever en las cláusulas contractuales los compromisos de ambas partes en el cumplimiento de procedimientos y protocolos para salvaguardar la SI.

11.11.2. Gestión de la prestación de servicios de proveedores

El supervisor de cada uno de los contratos debe hacerse responsable de monitorear el cumplimiento por parte del proveedor de las medidas en SI que quedaron pactadas. Para esto, la entidad debe contar con procedimientos estandarizados

11.12. Gestión de incidentes de seguridad de la información

11.12.1. Responsabilidades y procedimientos

Se deben tener documentados los procedimientos y los responsables para:

- Seguimiento, detección, análisis y reporte de eventos e incidentes de SI.
- Valoración y toma de decisiones sobre eventos de SI.
- Valoración de debilidades en SI.
- Planificación y preparación de respuesta a incidentes.

- Trazabilidad de las actividades de gestión de incidentes.
- Manejo de evidencia forense.

- Escalar el incidente a instancias superiores.

- Recuperación controlada de incidentes.

- Activar los canales de comunicación adecuados.

- Asegurar que el personal competente realice un manejo adecuado del incidente.

- Asegurar que se mantengan contactos apropiados con las autoridades, grupos de interés o foros relacionados con SI.

- Establecer el paso a paso a seguir en el caso de un evento de SI, (tomar nota inmediatamente, tales como violación a la SI o el tipo de no conformidad o, mal funcionamiento, mensajes en la pantalla y reporte inmediato al punto de contacto)

- Informar a la Dirección de Talento Humano los casos de violación de las políticas de Seguridad de la Información por parte de empleados y que están consignadas en el presente manual, dado que pueden dar lugar al debido proceso para la comprobación de faltas y establecimiento de sanciones disciplinarias conforme a lo establece el Reglamento Interno de Trabajo de LOTERÍA DE MEDELLIN.

- Retroalimentar debidamente a las personas que reportan eventos de SI una vez se le haya realizado el tratamiento correspondiente y el caso haya sido cerrado.

11.12.2. Reporte de eventos de seguridad de la información

Lotería de Medellín promoverá entre los funcionarios y terceros que usan los servicios y sistemas de información de la Entidad, para que reporten cualquier debilidad de seguridad en la información, relacionada con los medios de procesamiento, los sistemas de información, la plataforma tecnológica, los medios físicos de almacenamiento y las personas.

Normas para el reporte y tratamiento de incidentes de seguridad:

- Es responsabilidad de los funcionarios de Lotería de Medellín reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos en la mayor brevedad posible.

- En caso de conocer la pérdida o divulgación no autorizada de información clasificada ó reservada, los funcionarios deben notificarlo a profesional de Riesgos para que se registre y se le dé el trámite necesario.

- La Gerencia o a quien se delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades, o para hacer pronunciamientos oficiales ante entidades externas.

Los eventos de seguridad de la información se deben informar a través de la Mesa de ayuda, tan pronto como sea posible. La Oficina de las TIC deberá recopilar, documentar y tipificar los incidentes que reporten los usuarios. Esto debe incluir la violación de claves de acceso, la pérdida de información, el daño físico de archivos, la violación de la confidencialidad, ataques de hacking directos a la infraestructura, internos o externos, o cualquier otro incidente que ponga en riesgo la seguridad de la información.

Con el objetivo de tener claridad suficiente de cuando un evento es un incidente de SI, se deben definir los parámetros de confidencialidad, integridad y disponibilidad esperados y la violación de estos, en qué consisten los errores humanos que ponen en riesgo la SI, las no conformidades con las políticas de SI, el mal funcionamiento del software y el hardware, los cambios no controlados en los sistemas informáticos, y las violaciones de los acuerdos de seguridad física, de tal manera que se pueda identificar la diferencia cuando se presente una situación adversa.

En los casos en que se evidencie o se sospeche de qué se trata de un ataque malintencionado, interno o externo a la infraestructura tecnológica de la entidad, se deberá informar a la unidad de delitos informáticos de la policía nacional o su equivalente.

11.12.3. Reporte de debilidades de seguridad de la información

Eventos o características de los sistemas informáticos en los que se sospeche de la existencia de una debilidad o vulnerabilidad en la SI (por ejemplo lentitud inusual, reinicio frecuente, sospecha o posibilidad procedimental de ingreso no autorizado, violación de la confidencialidad, etc) deben ser reportadas a la Mesa de Ayuda para ser caracterizadas y valoradas por la Oficina de las TIC.

Adicionalmente, de acuerdo con el lineamiento LI.INF.13 del Marco de Referencia de la Arquitectura Empresarial para la Gestión de TI elaborado por Mintic, se deben generar mecanismos que permitan a los consumidores de los componentes de información reportar los hallazgos encontrados durante el uso de estos.

11.12.4. Evaluación de eventos de SI y decisiones sobre ellos

Todos los reportes de eventos de SI deben ser caracterizados, evaluados y valorados con el objetivo de determinar si se clasifica como incidente de seguridad y/o se requiere una acción de mitigación o de control.

11.12.5. Respuesta a incidentes de seguridad de la información

Una vez es caracterizado un evento de SI se debe proceder a la solución o mitigación de sus causas. Se debe disponer de procedimientos documentados para las acciones a tomar en cada caso, incluyendo la respectiva documentación del caso específico y, la comunicación a la personas claves de la entidad, y que pueden incluir además, análisis forense de SI, evaluación del monitoreo automático, escalamiento a instancias jerárquicas superiores, y el tratamiento de las vulnerabilidades conexas al incidente, todo dependiendo de las características del incidente.

11.12.6. Aprendizaje obtenido de los incidentes de SI

El historial completo de cada uno de los incidentes de SI debe ser documentado y almacenado en un repositorio único

11.12.7. Recolección de evidencia

Dentro del procedimiento de manejo de incidentes de SI se debe incluir la identificación, recolección y preservación de evidencias, las cuales deben custodiarse de manera adecuada con el objetivo de garantizar que no sean alteradas. Para situaciones excepcionales se debe consideras la seguridad de las personas involucradas en el evento.

11.13. Aspectos de seguridad en la continuidad del negocio

11.13.1. Planificación de la continuidad de la SI

Lotería de Medellín proporcionará los recursos suficientes para dar respuesta efectiva en caso de contingencia o eventos catastróficos que se presenten en la Entidad y que afecten la continuidad de su operación.

Consideraciones de seguridad de la información para la continuidad del negocio:

- Se deben identificar situaciones de emergencia o desastres para la Entidad, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.

- El profesional de Riesgos y La Oficina de las TIC deben participar de manera activa en los temas relacionados con la continuidad del negocio y la recuperación ante desastres.

- El profesional de Riesgos y La Oficina de las TIC deben realizar los análisis de impacto al negocio y los análisis de riesgos de continuidad, para posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.

- El profesional de Riesgos y la Oficina de las TIC, deben seleccionar las estrategias de recuperación más convenientes para la Entidad.

- El profesional de Riesgos debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.

- Los Jefes de las dependencias deben identificar y documentar al interior de sus áreas los procedimientos de continuidad que podrían ser utilizados en caso de un evento adverso, teniendo en cuenta la seguridad de la información.

La entidad debe contar con un BCP (Plan de Continuidad del Negocio) mediante el cual se prevean las posibles situaciones adversas que pongan en riesgo la operación de la entidad.

Este plan debe incluir un plan de contingencias informáticas que incluya al menos los siguientes puntos:

- Continuar con la operación del área con procedimientos informáticos alternos.

- Tener los respaldos de información en un lugar seguro, fuera del lugar en el que se encuentran los equipos.
- Tener el apoyo por medios magnéticos o en forma documental, de las operaciones necesarias para reconstruir los archivos dañados.

- Contar con un instructivo de operación para la detección de posibles fallas, para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.

- Contar con un directorio del personal interno y del personal externo de soporte, al cual se pueda recurrir en el momento en que se detecte cualquier anomalía.

- Ejecutar pruebas de la funcionalidad del plan.

- Mantener revisiones del plan a fin de efectuar las actualizaciones.

- Identificar y documentar los incidentes de seguridad de la información

Dentro del Plan de Continuidad del Negocio se debe tener previsto que en un escenario de activación de dicho plan, los mecanismos de contingencia deben contar con unas mínimas condiciones de SI que deben ser establecidas previamente de tal manera que no se ponga en riesgo la confidencialidad, integridad ni disponibilidad de la información.

11.13.2. Implementación de la continuidad de la SI

Para activar el BCP, la entidad debe contar con personal idóneo debidamente entrenado y sintonizado con los procedimientos documentados, tener establecidas los responsables de su activación y el área responsable de su monitoreo y actualización.

11.13.3. Verificación, revisión y evaluación de la continuidad de la SI.

Se deben realizar periódicamente pruebas de funcionamiento del plan de continuidad del negocio. Y se debe evaluar, documentar y verificar que no se incremente el riesgo en SI.

11.13.4. Disponibilidad de instalaciones de procesamiento de información.

El o los centros de datos que soporten la operación de la entidad, deben contar con una arquitectura redundante en sus principales componentes, de tal modo que se minimice la probabilidad de interrupción de los servicios respectivos. Se debe contar con procedimientos para realizar pruebas del funcionamiento de dicha arquitectura.

11.14. Cumplimiento

11.14.1. Identificación de la legislación aplicable.

Lotería de Medellín velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor, propiedad intelectual, la protección de los datos personales de sus clientes, proveedores y demás terceros de los cuales reciba y administre información.

Consideraciones de cumplimiento:

- La Oficina de las TIC debe certificar que todo el software que se ejecuta 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.

- La Oficina de las TIC debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo para el desarrollo de las actividades laborales.

- En cumplimiento de la de Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, la Oficina Jurídica velará por la protección de los datos personales.

- Los usuarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información clasificada y/o reservada de la Entidad o de los funcionarios en el ejercicio de sus funciones.

11.14.2. Derechos de propiedad intelectual

Con el fin de dar cumplimiento a las normas legales sobre propiedad intelectual y derechos de autor, en Lotería de Medellín se deben tener en cuenta los siguientes lineamientos:

- Todos los derechos de propiedad intelectual de los productos, servicios y aplicaciones que hayan sido diseñados, desarrollados o modificados por empleados o personal subcontratado son de propiedad exclusiva de Lotería de Medellín.

- Se debe instalar solo software que esté licenciado por Lotería de Medellín. En caso de tratarse de un software en demostración, es necesario contar con un documento de autorización del fabricante o distribuidor autorizado y la aprobación de la Oficina de las TIC.

- No se debe instalar, copiar software o utilizarlo en beneficio propio o de terceros al igual que reproducirlo sin autorización. El software que es licenciado para Lotería de Medellín o es de su propiedad, solo podrá ser instalado en los computadores de la misma.

- Cualquier reproducción a que hubiere lugar solo se hará para uso exclusivo de Lotería de Medellín y únicamente bajo estricto cumplimiento de los acuerdos de uso que se encuentran vigentes con los fabricantes y proveedores de tales programas.

11.14.3. Protección de registros.

La entidad debe contar con un plan de gestión documental que incluya tablas de retención documental. Se debe disponer de un procedimiento para la validación y monitoreo del cumplimiento de dicho plan, incluyendo las características del almacenamiento, tiempos de

retención, gestión de metadatos, herramientas de búsqueda y recuperación de documentos, entre otros factores relevantes.

11.14.4. Protección y privacidad de los datos personales.

Lotería de Medellín se compromete con el cumplimiento de la Ley 1581 de 2012 y su decreto reglamentario 1377 de 2013. Esto incluye:

- Mecanismos de notificación al titular de los datos y la aceptación por parte de este del tratamiento de los datos personales por parte de la entidad.

- Implementación por parte de la entidad de los mecanismos tecnológicos y procesos necesarios para garantizar la adecuada protección de los datos personales, haciendo énfasis en los datos sensibles, en especial en los relacionados con la salud de los afiliados.

Adicionalmente, de acuerdo con el lineamiento LI.INF.14 del Marco de Referencia de la Arquitectura Empresarial para la Gestión de TI generado por Mintic, La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe incorporar, en los atributos de los Componentes de información, la información asociada con los responsables y políticas de la protección y privacidad de la información, conforme con la normativa de protección de datos de tipo personal y de acceso a la información pública.

11.14.5. Revisión independiente de la seguridad de la información

La Dirección de Gestión Control debe contar con planes, metodologías y procedimientos para la realización de auditorías anuales que evalúen los avances en seguridad de la información y la implementación del MSPI en la entidad.

11.14.6. Cumplimiento de las políticas y normas de seguridad.

Todos los directivos de Lotería de Medellín deben realizar revisiones periódicas del cumplimiento, por parte del personal a cargo, de las políticas y normas internas en SI. Para esto se deben elaborar planes y procedimientos para el monitoreo, y la documentación de los respectivos hallazgos, de tal manera que surjan respectivos planes de mejoramiento.

11.14.7. Revisión de cumplimiento técnico.

Las políticas de seguridad de la información, deben ser cumplidas por todos los integrantes que hacen parte de Lotería de Medellín, por lo tanto, el incumplimiento de las normas aquí estipuladas pueden acarrear acciones disciplinarias y/o legales.

La Oficina de las TIC deberá velar por el cumplimiento de todas las políticas de seguridad y realizar monitoreo permanente a la evolución de la aplicación del Modelo de Seguridad y Privacidad de la Información en la entidad.

11.14.8. Monitoreo y uso de los sistemas

Se debe establecer los mecanismos adecuados para detectar las actividades que amenacen la seguridad de la información. Para tal fin se deben tener en cuenta los siguientes lineamientos:

- Lotería de Medellín se reserva el derecho de interceptar o vigilar cualquier tráfico de información que pase a través de las redes de comunicaciones y sistemas de información como parte de sus actividades de vigilancia, mantenimiento, investigación, auditoría o seguridad del desempeño del sistema. Todo el personal debe estar consciente de esto cuando use los sistemas de información de Lotería de Medellín.

- De acuerdo con el lineamiento LI.SIS.23 del Marco de Arquitectura Empresarial para la Gestión de TI emitido por Mintic, todas las aplicaciones y servicios críticos que hacen parte de la infraestructura de comunicaciones, seguridad y procesamiento de información deben proporcionar logs (registros) para permitir el seguimiento y trazabilidad de las actividades de los administradores, y usuarios en general.

- De acuerdo con el lineamiento LI.INF.15 del Marco de Referencia de la Arquitectura Empresarial para la Gestión de TI emitido por Mintic, se deben definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los componentes de información. Estos mecanismos deben ser considerados en el proceso de gestión de dichos componentes. Los sistemas de información deben implementar los criterios de trazabilidad y auditoría definidos para los componentes de información que maneja.

- El jefe inmediato deberá notificar a la Dirección de Talento Humano el incumplimiento de las políticas de Seguridad de la Información por parte de algún empleado a su cargo.

- La Oficina de las TIC debe realizar, al menos 1 vez por año, los servicios de test de penetración e identificación de vulnerabilidades, así como documentar los hallazgos, realizar las actividades de remediación que le recomienden y hacer seguimiento a los avances en ese aspecto.

12. Indicadores de seguridad de la información.

Para medir el avance en la implementación del Modelo de Seguridad y Privacidad de la Información, se cuenta con el indicador “Porcentaje de avance en la implementación del Modelo de Seguridad y Privacidad de la Información” que se obtiene mediante la siguiente fórmula:

Porcentaje de avance en la implementación del Modelo de Seguridad y Privacidad de la Información= Promedio de los porcentajes de cada uno de los 14 dominios (sección Políticas Específicas)

Los porcentajes de cada dominio se obtienen promediando cada uno de los porcentajes de los respectivos controles.

13. Referencias

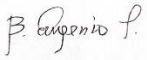
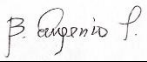
- NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC Colombiana 27001:20013. 2013-12-11. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos
- ELABORACIÓN DE LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Mintic. Versión 1. 11/05/2016.
- GUIA PARA LA GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN. Mintic. 2016.
- GUÍA PARA LA CALIFICACIÓN DE LA INFORMACIÓN DE ACUERDO CON SUS NIVELES DE SEGURIDAD. Presidencia de la República. 2017
- LINEAMIENTOS DEL MARCO DE REFERENCIA DE ARQUITECTURA EMPRESARIAL PARA LA GESTIÓN DE TI. Mintic Versión 1.1 Mayo 11 de 2017
- http://www.iso27000.es/glosario.html. Recopilado el 12 de enero de 2021.
- https://www.wikipedia.org/. Consultas realizadas el 12 de enero de 2021.

14. Responsables de la Política

Generación de la Política: Oficina de las TIC

Actualización, socialización y verificación del cumplimiento de la política: Oficina de las TIC

Autorizador de la Política: Gerente de Lotería de Medellín.

	NOMBRE	CARGO	FIRMA
Proyectó	B. Eugenio Londoño U	Jefe Oficina de las TIC	
Aprobaron	B. Eugenio Londoño U	Jefe Oficina de las TIC	
	David Mora	Gerente Lotería de Medellín	
Los abajo firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales y por lo tanto bajo nuestra responsabilidad lo presentamos para firma			

Elaboró: Oficina Tics	**Revisó:** Oficina de Planeación	**Aprobó:** Director TIC´s
Fecha: 12/01/2021	**Fecha:** 12/01/2021	**Fecha:** 26/03/2021