2021

POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

SISTEMAS

LOTERIA DEL CAUCA

31-3-2021

POLÍTICAS DE SEGURIDAD DE LA INFORMACION

La información escrita y/o impresa en papel, almacenada electrónicamente, compartida, salvaguardada en espacios físicos o virtuales, o transmitida por medios electrónicos; es un componente indispensable en la conducción y consecución de los objeticos corporativos de la lotería del Cauca definidos por la estrategia de la empresa, razón por la cual es necesario establecer un marco en el cual se asegure que la información es protegida contra una amplia gama de amenazas de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada, compartida, comunicada o almacenada.

Las políticas de seguridad de la información tienen por objeto establecer medidas y patrones técnicos de administración y organización de las tecnologías de la información y las comunicaciones TIC's de todo el personal comprometido en el uso de los servicios informáticos proporcionados por la lotería del Cauca.

DEFINICIONES USADAS EN LAS POLÍTICAS DE SEGURIDAD

- Access point (punto de acceso): equipo electrónico que actúa como punto central de conexión para los equipos que van a acceder a la red inalámbrica. Utilizan antenas para transmitir y recibir la información que los usuarios soliciten.
- Autenticación: el proceso de asignar el permiso al usuario para manejar los objetos que solicita.

- Aplicaciones: Son programas informáticos que tratan de resolver necesidades concretar del usuario, como por ejemplo: escribir, dibujar, escuchar música.

- Backup o copia de seguridad: Copia de los archivos y aplicaciones hechos para evitar pérdidas de información y facilitar la recuperación en los casos de caída del sistema.

- Directorio Activo: Es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

- Dispositivos Extraíbles: Un dispositivo de almacenamiento extraíble es una unidad que te permite almacenar datos para después usarlos en cualquier ordenador, y transportarlos de manera ligera, ya que su tamaño es reducido. Podemos distinguir diferentes tipos de dispositivos extraíbles de almacenamiento como son:
  - ✓ Discos ópticos (CD, DVD, Blu-ray).
  - ✓ Memorias USB.
  - ✓ Discos duros externos.
- Equipo de Computo: Son todos los equipos de cómputo electrónicos que pertenecen a la compañía: Computadoras, CPU, Monitores, Teclados, Mouse, Servidores, Drivers, Scanner, etc.
- Hardware: Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

- Infraestructura inalámbrica: todos los componentes involucrados para conformar una red inalámbrica. Por ejemplo: puntos de acceso, antenas, cableado, etc.

- Información: Toda información, independientemente de su forma, que es creada, almacenada o procesada por los recursos de información, redes de comunicaciones y datos o medios de almacenamiento.

- Privacidad: confidencialidad de la información que se transmite por la red.

- Proceso de sistemas: Área de la Lotería del Cauca, responsable de los recursos de información, así mismo de construir y diseñar las políticas necesarias para el adecuado uso y aseguramiento de la información generada en la Empresa y tratada electrónica o digitalmente.

- Red inalámbrica: una red de comunicaciones que utiliza el aire, minimizando la necesidad de cables, para trasmitir y recibir datos.

- Recursos de Información (RI): Todo equipo de cómputo, impresiones, recursos en línea, medios de almacenamiento magnético y todas las actividades relacionadas a sistemas de cómputo, incluyendo cualquier dispositivo capaz de recibir e-mails, navegación en la Web, o con capacidad de recepción, almacenamiento, manejo, o transmisión electrónica de datos, por ejemplo y no limitado a, servidores, computadores personales, computadores portátiles, computadores de mano, asistentes personales portátiles (PDA), Smart phone, sistemas de procesamiento distribuido, redes de datos, recursos de telecomunicación, teléfonos, equipos de fax e impresoras. Adicionalmente, son considerados como Recursos de Información: los procedimientos, los equipos, instalaciones físicas, software,

y data que sean diseñados, producidos, operados y mantenidos para crear, recolectar, grabar, procesar, almacenar, recuperar, desplegar y transmitir información.

- SSID: identificación que transmite los puntos de acceso referente al nombre dado a la red inalámbrica para identificar el servicio.

- Software: Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

- Sistemas Operativos: Tienen como misión que el ordenador gestione sus recursos de forma eficiente, además de permitir su comunicación con el usuario. Como por ejemplo el Sistema Windows.

- Servicio: Prestación de un beneficio, tarea o proceso a los diferentes usuarios, un proceso que corre en un servidor de manera permanente.

- Usuario: Tiene la responsabilidad de 1.- usar los recursos sólo para los propósitos establecidos por la Lotería del Cauca, 2.- cumplir con los controles establecidos por la empresa, y 3.- prevenir declaraciones de información confidencial o sensible. El usuario es la persona que ha sido autorizada para leer, ingresar o actualizar información por la empresa la cual es la propietaria de la información. El usuario cumple el más simple control efectivo para proveer adecuada seguridad.

- Conexión remota: aplicaciones de escritorio remoto las cuales permiten controlar un computador desde otro dispositivo, que puede ser otro computador, donde también se debe tener instalada la misma aplicación,

estas herramientas facilitan el trabajo a quienes se dedican al soporte técnico y también aportan beneficios para aquellos que trabajan a distancia

- Transformación Digital: Es el cambio asociado con la aplicación de tecnologías digitales en todos los aspectos de la sociedad humana.

A continuación se nombran las políticas de seguridad de la información recomendadas para el proceso de apoyo de sistemas de la Lotería del Cauca, de acuerdo con las recomendaciones hechas basadas en la norma ISO 27001.

1. Política de seguridad de la información.
2. Política de uso de los recursos de la empresa.
3. Política de administración y uso de cuentas de correo
4. Política de administración de contraseñas.
5. Política de administración y seguridad en servidores.
6. Política de administración de directorio activo.
7. Política de administración de incidentes técnicos.
8. Política de respaldo y restauración de información.
9. Política de uso de dispositivos de almacenamiento extraíbles.
10. Políticas de uso de redes y acceso a internet.
11. Política de licenciamiento y soporte de software.
12. Política de conexión remota.(trabajo en casa)

1.- POLÍTICA DE SEGURIDAD DE INFORMACIÓN

ALCANCES

Las políticas de seguridad de la información se aplican a toda información obtenida, creada, o administrada por la Lotería del Cauca, dentro de sus recursos de Información. Estas políticas y estándares están basadas en la interpretación del estándar ISO 27001, y se aplican igualmente a todos los niveles de gerencia y personal, adicionalmente, ésta política se aplica a toda la información generada por las funciones de recursos de Información la Lotería del Cauca, durante el tiempo de transferencia hacia un agente externo de la empresa o durante su propia disposición y destrucción.

AUDIENCIA

Estas Políticas se aplican igualmente a todo el personal de la lotería del Cauca y a todos los usuarios externos/contratistas autorizados a acceder a los recursos de Información de la empresa.

APLICACIÓN

La Lotería del Cauca, protegerá todos sus recursos de Información de la empresa de acuerdo a políticas definidas.

Específicamente, la empresa aplicará políticas, procedimientos, prácticas estándares, y guías para proteger las funciones de los RI (Recursos de Información) de datos internos, errores de programación, mal manejo por funcionarios dentro de o fuera de la empresa. Esto con la finalidad de proteger a la empresa de riesgos que comprometan la integridad de los programas, violación de los derechos

individuales a la privacidad y confiabilidad, violación del derecho penal, o de potenciales daños a la seguridad pública.

Todos los programas de seguridad de los recursos de información de la empresa serán responsables y adaptables a los cambios tecnológicos que afecten los recursos de Información.

VIOLACIONES

Cualquier evento que resulte en robo, pérdida o uso desautorizado, declaración no autorizada, modificaciones desautorizadas, destrucciones desautorizadas, o acceso a RI denegados, constituyen una brecha de seguridad y confidencialidad. Estas violaciones pueden incluir, pero no limitarse, a los siguientes:

- Exponer a la empresa a actuales o potenciales pérdidas monetarias comprometiendo la seguridad de los RI.
- Involucra las declaraciones de información sensible o confidencial o el uso no autorizado de datos o recursos de la empresa.
- Incluye el uso de los RI para beneficio personal, no ético, dañino o con propósitos ilícitos.

ACCIONES DISCIPLINARIAS

La Violación de estas Políticas pueden resultar en acciones disciplinarias inmediatas, pero no limitadas a:

- Amonestaciones Formales

- Suspensión o acceso restringido a los Recursos de Información de la empresa
- Restitución o indemnización por cualquier daño o apropiación ilícita de cualquier propiedad de la empresa
- Suspensión de labores
- Suspensión de conexión remota
- Término de contrato
- Despido
- Proceso Civil o Penal.

POLÍTICAS

1) Los controles de Seguridad de los RI no deben ser obviados o inutilizados.
2) La conciencia de seguridad del personal debe ser continua, reforzada, actualizada y validada.
3) Todo el personal es responsable por el manejo del uso de los RI y son responsables por los actos relacionados a la seguridad de los RI. El personal es igualmente responsable de reportar cualquier sospecha o confirmación de violaciones o manejo inapropiado de las políticas de seguridad de información.
4) Las contraseñas, números de identificación de personal (PIN), claves de seguridad (tarjeta inteligente de seguridad), y otros procedimientos y dispositivos de seguridad en los sistemas de informáticos deben ser protegidos por el usuario. Toda violación de seguridad debe ser reportada al responsable o gerente encargado y/o al área de sistemas.
5) El Acceso, el cambio y el uso de los RI deben ser estrictamente seguros. La autorización para acceso a la información para cada usuario debe ser revisada regularmente, así como el cambio de status del trabajador como:

transferencia, promoción, baja o culminación de sus actividades.

6) El uso de los RI debe ser oficialmente autorizado, los mismos que son sólo para propósitos de la empresa. No existe garantía de privacidad personal o acceso a herramientas, pero no limitada a: e-mail, navegación en Internet, y otras herramientas de discusión electrónica. El uso de estas herramientas de comunicación electrónica puede ser monitoreado para realizar o esclarecer reclamos o procesos de investigación. Los departamentos o áreas que tienen a cargo el manejo de computadores, deben ser responsable de la adecuada utilización de los RI, el efectivo manejo del mismo, y de reportar su estado y manejo.
7) Cualquier información utilizada en un sistema de los RI, debe ser mantenida con confidencialidad y seguridad por el usuario. El hecho de que la información sea almacenada electrónicamente no cambia el requerimiento de mantener la información segura y confiable. Más bien, el tipo o clasificación de la información por si misma es la base para determinar si la información debe guardarse en forma confidencial y segura. Adicionalmente, si esta información es almacenada en un papel o un formato electrónico, o si la información es copiada, impresa o trasmitida electrónicamente debe ser protegida como confidencial y segura.
8) Al término de la relación de trabajo con la empresa, los usuarios deben entregar todos los bienes y RI asignados por la empresa. Se deben aplicar todas las políticas de seguridad de los RI y relacionadas con el evento de culminación de relaciones laborales hasta que la devolución sea realizada. Asimismo, esta política da por terminada toda relación.
9) El responsable del proceso de sistemas es el encargado de argumentar a la alta gerencia y recibir su aprobación para la elaboración de cualquier proyecto de adquisición de hardware, compra o desarrollo de software para la empresa. Los costos de las adquisiciones, desarrollo y operación

del hardware y aplicaciones, deben ser autorizados por los Gerentes o Directores apropiados. La Gerencia y los departamentos solicitantes deben actuar dentro de sus límites de aprobaciones de acuerdo con las políticas de autorización de compras de la empresa.

10) El departamento o área que requiera o autorice una aplicación de computador, debe cumplir con los pasos apropiados para asegurar la integridad y seguridad de todos los programas y archivos de información creados u obtenidos por las aplicaciones de cómputo.

11) La red de RI es de propiedad y controlada por el proceso de sistemas. Las aprobaciones deben ser obtenidas del área de sistemas y tecnología antes de conectar a la red un recurso que no cumpla con las guías o estándares de la red publicados. El área de sistemas se reserva el derecho de remover de la red cualquier recurso que no cumpla con los estándares o que no sean considerados como adecuadamente seguros.

12) La venta o alquiler de aplicaciones de cómputo o datos, incluyendo lista de e-mail y directorios telefónicos, a otras personas o organizaciones debe cumplir con todas las políticas y procedimientos legales y fiscales de la empresa.

13) La integridad del uso general de software, utilidades, sistemas operativos, redes y archivos de información, son responsabilidad de cada área de la empresa. Los datos para pruebas y con propósitos de investigación deben ser autorizados por el responsable del proceso de sistemas.

14) Todos los cambios o modificaciones en los sistemas de RI, redes de datos, programas o datos deben ser aprobados por el departamento encargado el cual es responsable de su integridad.

15) El proceso de sistemas debe proveer controles de accesos adecuados para monitorear los sistemas y proteger la información y programas de malos manejos de acuerdo con las necesidades definidas por los

propietarios o usuarios. El acceso debe estar correctamente documentado, autorizado y controlado.

16) Todos los departamentos o áreas deben evaluar cuidadosamente los riesgos de cambios desautorizados, declaraciones desautorizadas, o pérdida de los datos de los que son responsables, y asegurar a través del uso de sistemas de monitoreo, que a empresa esté protegida contra daños u otros. Administrador de las aplicaciones y el área de sistemas y tecnología deben contar con un backup apropiado y planes de contingencia para así contrarrestar desastres o riesgos de daños o perjuicios basados en los requerimientos de la empresa.

17) Todos los contratos de sistemas o aplicaciones de cómputo, alquiler, licencias, u otros acuerdos deben ser autorizados y firmados por el gerente y/o usuario autorizado de la empresa, y debe contener los términos aprobados por el departamento legal, notificando a los proveedores o contratistas para los RI de la empresa, el respetar los derechos de propiedad de los sistemas de información, programas, y datos requeridos.

18) Los sistemas de cómputo de los RI y equipos asociados, utilizados para los fines de la empresa, y que son operados y administrados fuera del control de la empresa, deben cumplir requerimientos contractuales y estar sujetos a monitoreo.

19) El acceso externo desde y hacia los RI deben cumplir las guías de seguridad apropiadas y publicadas por la empresa.

20) Todo software comercial utilizado en los sistemas de cómputo debe contar con acuerdos de licencias de software, que describa los derechos de uso y las restricciones del producto. El personal debe cumplir con todas los acuerdos de licencias y no debe realizar copias ilegales del software. El área de Informática se reserva el derecho de remover cualquier software sin licencia de los RI.

21) El área de Informática se reserva el derecho de remover cualquier software o archivos de cualquier sistema e cómputo, no relacionado con el negocio o fines de la empresa. Ejemplos de este software son: juegos, programas de mensajería o chat, pop e-mail, archivos de música, fotos, freeware y shareware.

22) Las adherencias a todas las otras políticas, prácticas estándar, procedimientos y guías utilizadas, como soporte de esta política de Seguridad de Información, es obligatoria.

2.-POLÍTICA DE USO DE LOS RECURSOS DE LA EMPRESA

PROPÓSITO

El propósito principal de esta política es crear una cultura en los funcionarios de la Lotería del Cauca, para que realicen un correcto uso de los recursos informáticos asignados al momento de ingresar a desarrollar su actividad laboral.

AUDIENCIA

Esta política aplica para todos los funcionarios de la Lotería del Cauca con contrato laboral vigente.

POLÍTICAS

1) El área de apoyo de sistemas de la Lotería del Cauca debe poner a disposición la información de equipos de cómputo, aplicaciones de software, así como los servicios de soporte y mantenimiento requeridos para el normal desempeño de las funciones.

2) El proceso de sistemas será quien valide el cumplimiento de las condiciones técnicas de los equipos informáticos y aplicaciones de software adquiridos por la empresa.
3) El proceso de sistemas tendrá bajo su resguardo las licencias de software, CD de software y manuales originales y respaldos de instalación.
4) Los requerimientos de equipos de cómputo, se llevarán a cabo mediante la solicitud y justificación por escrito, firmada por el Jefe del Área solicitante, lo cuales serán evaluados por el área de sistemas para su autorización y posterior compra.
5) El proceso de sistemas es encargado de tramitar las asignaciones, reasignaciones y bajas, de equipos de cómputo ante el área encargada de los inventarios de activos.
6) Queda prohibido a los usuarios mover los equipos de cómputo por su propia cuenta, el usuario deberá solicitar al área de sistemas, así como informar la razón del cambio y en su caso, requerir la reasignación del equipo.
7) El área de sistemas informará a la oficina de recursos físicos la salida de algún recurso informático el cual requiera ser trasladado fuera de las instalaciones de la empresa por motivo de garantía, reparación o cualquier otro evento.
8) Queda prohibido instalar software no autorizado o que no cuente con licencia en estaciones de trabajo por personal distinto al perteneciente al área de sistemas y este debe realizarlo bajo los estándares adecuados.
9) Cada equipo está preparado con el Hardware y Software necesario para su funcionamiento, el usuario no deberá alterar el contenido físico y/o lógico.
10) En caso de presentar una falla física o lógica se deberá notificar al área de sistemas para su revisión y/o reparación de acuerdo al procedimiento establecido.

11) En ningún caso el usuario intentará reparar el equipo ó diagnosticarlo, únicamente informar de la posible falla.
12) El usuario será el único responsable del equipo de cómputo.
13) En ningún caso, el usuario tendrá cerca alimentos, bebidas u otros materiales que puedan derramarse sobre el equipo.
14) Solo se utilizará el equipo para funciones de interés del área y de ninguna manera para asuntos personales.
15) Dado el caso de que el usuario no tenga conocimientos y/o experiencia en el manejo de equipos de cómputo lo notificará al área de sistemas para su correspondiente Capacitación.
16) El software no puede ser utilizado por el usuario para realizar trabajos personales.
17) El análisis de la necesidad de la adquisición o desarrollo de software será realizado por el proceso de sistemas, y la autorización de adquisición / compra por el comité de compra y la alta dirección.

Acuerdo de responsabilidad y buen uso de los recursos de Información de la Lotería del Cauca

En mi calidad de Funcionari@ de la Lotería del Cauca, declaro conocer la responsabilidad que me impone haber recibido el derecho a utilizar los recursos de cómputo, facultad que me fue conferida única y exclusivamente para el cumplimiento de las funciones asignadas a mi cargo. Me obligo a utilizar este derecho solamente, mientras esta autorización este vigente y siempre de acuerdo con las normas de la lotería del Cauca.

Comprendo y acepto el carácter personal, secreto e intransferible de mis contraseñas y cuentas de acceso a los sistemas de cómputo de la lotería del Cauca que me han sido asignados y me comprometo a no divulgarlo verbalmente o por escrito a persona alguna. Así mismo, en su utilización emplearé mi mejor criterio.

Estoy de acuerdo que NO debo utilizar los recursos de Información que me fueron asignados en actividades ilegales, criminales, no éticas ó irregulares como intimidar, insultar o molestar a otros, en todo momento respetare la intimidad, confidencialidad y derechos individuales de los demás.

NO utilizaré las facilidades del correo electrónico para el envío masivo de materiales molestos, obscenos, ilegales o innecesarios.

Acepto el presente acuerdo como parte integrante a la relación laboral con la empresa y el no cumplimiento de lo aquí consignado será considerado FALTA GRAVE.

Acepto todas las políticas de seguridad de la información relacionadas en este documento.

Para constancia fue firmado este documento el día _____ del mes de _____ de 20___

_____

Nombre Funcionario
CC. de.

3.-POLÍTICA DE ADMINISTRACIÓN Y USO DE CUENTAS DE CORREO

PROPÓSITO

El propósito de esta política de manejo de cuentas de correo es establecer las reglas para la creación, monitoreo, control y remoción de cuentas de usuarios.

AUDIENCIA

La política de manejo de cuentas de correo se aplica a todos los funcionarios con acceso autorizado a recursos informático de la empresa.

POLÍTICAS

1) Todas las cuentas creadas deben pertenecer a funcionarios con vinculación laboral vigente, las cuentas de correo genéricas su creación debe ser solicitada por y aprobado por la dirección de recursos humanos.
2) Todas las cuentas de usuario asignado deben identificarse usando la primera letra inicial del primer nombre seguido del primer apellido del funcionario con dominio @loteriadelcauca.gov.co
3) La contraseña asignadas a una cuenta por primera vez la realizará el área de sistemas en el momento de la creación, obligatoriamente debe ser cambiada inmediatamente por el usuario en su primer acceso a la cuenta de correo convirtiéndose en su responsabilidad.
4) Todas las cuentas tienen una contraseña con caducidad de 90 días, al término del tiempo la plataforma solicitará el cambio de la contraseña; No se admite la repetición de contraseñas, debe tener una longitud mínima de 8 caracteres con un carácter en mayúscula o caracteres especiales y números.

5) El administrador del servidor Profesional Universitario Grado 01 de sistema es responsable y no limitante de:

- ✓ Crear, modificar y remover las cuentas de los funcionarios de la empresa, funcionarios que ya no posean relación laboral con esta.
- ✓ Deben tener un proceso documentado para modificar una cuenta de usuario, con el fin de afrontar situaciones tales como cambio de nombres, cambio de cuentas y cambio de perfil.
- ✓ Son sujeto a revisiones de auditoría independiente.
- ✓ Deben tener un procedo documentado/o en plataforma para la revisión y validación periódica de las cuentas existentes.
- ✓ Deben cooperar con el personal autorizado encargado de investigar incidentes de seguridad.

6) El administrador de la plataforma es el responsable de crear la cuenta, entregar la contraseña por primera vez al usuario el cual debe cambiarla en su primer acceso a la cuenta, una vez cambiada el área de sistemas no tiene acceso a identificar la contraseña, en caso de pérdida u olvido el funcionario debe realizar el cambio de contraseña nuevamente.

7) NO se utilizará las facilidades del correo electrónico para el envío de materiales molestos, obscenos, ilegales o innecesarios.

8) Cada cuenta de correo representa una cuenta institucional, por lo tanto debe ir finalizada con la firma la cual se adjunta al final de todos los mensajes salientes de cada funcionario conservando identidad y homogeneidad empresarial :

Tipo de Letra….. ARIAL 11

1er NOMBRE 2º.NOMBRE 1er Apellido 2º. Apellido
Cargo
Dependencia a la que pertenece
LOTERIA DEL CAUCA

Cra.7 # 1N-66 Edificio Lotería del Cauca
Popayán-Colombia
PBX (2) 8233856 EXT xxx al cual pertenece
www.loteriadelcauca.gov.co
Twitter: @lotecauca-Facebook: Lotecauca

ACCIONES DISCIPLINARIAS

La violación de esta política puede resultar en acciones disciplinarias que puede dar término a contrataciones de funcionarios; término de la relación laboral en el caso de contratistas o consultores; o suspensión o expulsión en el caso de un practicante. Adicionalmente los funcionarios están sujetos a perder el acceso a los privilegios, e iniciar un proceso civil y/o penal.

4.-POLÍTICA DE ADMINISTRACIÓN DE CONTRASEÑAS

PROPÓSITO

El propósito de esta política de administración de contraseñas es establecer las reglas para la creación, distribución, protección y terminación de los mecanismos de autenticación de usuarios dentro de los recursos informáticos de la empresa.

AUDIENCIA

La política de administración de contraseñas se aplica a todos los funcionarios con acceso autorizado a cualquier recurso informático de la empresa.

POLÍTICAS

1) Todas las contraseñas deben contener letras mayúsculas, minúsculas, números, caracteres especiales y una longitud mínima de 8 caracteres.
2) El uso de información personal en la creación de una contraseña es considerado como peligroso.
3) Las contraseñas deben cambiarse periódicamente, la plataforma está programada automáticamente para solicitar el cambio de contraseña cada 90 días, No se admite la repetición de contraseñas.
4) La contraseña asignada a un usuario debe cambiarse la primera vez que sea utilizada por este.
5) Las contraseñas asignadas a cada usuario no deben ser divulgadas o compartidas con nadie.
6) Si la seguridad de una contraseña está en duda, la contraseña debe ser cambiada inmediatamente.
7) Las contraseñas para equipos de red como routers y swiches por defecto, deben ser cambiadas, documentadas y administradas solo por el personal del proceso de sistemas.

ACCIONES DISCIPLINARIAS

La violación de esta política puede resultar en acciones disciplinarias que puede dar término a contrataciones de funcionarios; término de la relación laboral en el caso de contratistas o consultores; o suspensión o expulsión en el caso de un practicante. Adicionalmente los funcionarios están sujetos a perder el acceso a los privilegios, e iniciar un proceso civil y/o penal.

5.-POLÍTICA DE ADMINISTRACIÓN Y SEGURIDAD EN SERVIDORES

PROPÓSITO

El propósito de la política de administración y seguridad en servidores es proporcionar un nivel de seguridad y control sobre el acceso, gestión y administración de los servidores de la lotería del Cauca.

AUDIENCIA

La política de administración y seguridad en servidores se aplica al Profesional Universitario Grado 01 Responsable del área de sistemas.

POLÍTICAS

1) Diseño de una hoja de vida para cada servidor, donde se incluya:

- ✓ Características del equipo, seriales, nombre del responsable del equipo,
- ✓ Necesidades del entorno de operación como circuito regulado al que pertenece, ups que lo respalda, temperatura y humedad.
- ✓ Documentación de configuración, instalación, actualizaciones del sistema operativo y software instalado.
- ✓ Registros de mantenimiento físico y lógico (Maquina, sistema operativo y aplicaciones instaladas).

2) La administración de los servidores debe ser realizada de forma exclusiva por el Profesional Universitario Grado 01 Responsable del proceso de sistemas o personal autorizado.

3) Realización de monitoreo constante de los servicios que presta el servidor, corroborando su correcto funcionamiento y la disponibilidad de acceso controlado a los usuarios.
4) Los servidores debe estar conectado a una fuente regulada de corriente, alejado de cualquier acceso físico no autorizado. Su ubicación debe hacerse en áreas seguras, de acceso controlable, ordenadas, limpias y protegidos contra agua, polvo, humedad, calor o cualquier amenaza natural o industrial que afecte su funcionamiento.
5) Realización de constante registro de eventos e incidentes, y la solución implementada.
6) Garantizar que quede registro del acceso y actividad realizada, en cada servidor.

ACCIONES DISCIPLINARIAS

La violación de esta política puede resultar en acciones disciplinarias que puede dar término a contrataciones de funcionarios; término de la relación laboral en el caso de contratistas o consultores; o suspensión o expulsión en el caso de un practicante. Adicionalmente los funcionarios están sujetos a perder el acceso a los privilegios, e iniciar un proceso civil y/o penal

6.-POLÍTICA DE ADMINISTRACIÓN DE DIRECTORIO ACTIVO

PROPÓSITO

La política de administración de directorio activo en servidores para creación de usuarios y contraseñas de equipos en la entidad, es establecer las reglas que

permitan tener un correcto uso de esta herramienta, es función específica del Profesional Universitario Grado 01 Responsable del área de sistemas.

AUDIENCIA

La política de administración del directorio activo aplica a todos los usuarios y equipos que poseen una cuenta o están registrados en el directorio activo de la empresa otorgando el acceso y creado su usuario y contraseña por el Responsable del área de sistemas, Profesional Universitario Grado 01.

POLÍTICAS

1) El servicio de directorio activo debe contar con la infraestructura y mecanismos que garanticen su disponibilidad en todo momento.
2) Los usuarios deben contar con claves dentro del directorio activo que garanticen el control de sus cuentas, estas claves deben contar con la seguridad de acuerdo a la política de administración de contraseñas.
3) El acceso al servidor de directorio Activo debe ser realizado únicamente por el responsable del área de sistemas Profesional Universitario Grado 01, del proceso de sistemas y de forma remota, debe contar con claves de alta seguridad, las cuales deben ser cambiadas periódicamente para evitar que sean copiadas o distribuidas a personal no autorizado.
4) El responsable del proceso de sistema u otros designados y autorizados del área.

- ✓ Son responsables de establecer los mecanismos, procesos y actividades que garanticen su disponibilidad en todo momento.
- ✓ Son responsables de establecer los permisos, limitaciones, restricciones y controles de acceso de los usuarios que hacen parte del directorio activo.

- ✓ Deben agregar, eliminar o modificar la información de los usuarios antiguos y nuevos.

ACCIONES DISCIPLINARIAS

La violación de esta política puede resultar en acciones disciplinarias que puede dar término a contrataciones de funcionarios; término de la relación laboral en el caso de contratistas o consultores; o suspensión o expulsión en el caso de un practicante. Adicionalmente los funcionarios están sujetos a perder el acceso a los privilegios, e iniciar un proceso civil y/o penal.

7.-POLÍTICA DE ADMINISTRACIÓN DE INCIDENTES TECNICOS

PROPÓSITO

El propósito de la política de administración de incidentes técnicos es brindar el soporte documental para gestionar de forma organizada y rápida la solución a incidentes que causen interrupción en la labor de los funcionarios de la lotería del Cauca, relacionados con recursos informáticos.

AUDIENCIA

La política de administración de incidentes técnicos se aplica a todos los funcionarios que su labor dependa de recursos informáticos como computadoras, teléfonos, impresoras o servicios de red o en servidores.

POLÍTICAS

1) Se debe documentar cualquier incidente, así como su solución, esto debe ser organizado y archivado como fuente referencial para futuros incidentes.
2) Adoptar medidas de seguridad eficientes que protejan los activos más críticos.
3) Documentar y clasificación de incidentes y sus respectivos tiempos de respuesta.
4) Planeación, implementación y documentación de procedimientos a posibles incidentes que afecten la información de la empresa.
5) Cada vez que se sospeche, ocurra o se confirme algún incidente de seguridad, tales como virus, gusanos, descubrimiento de intrusiones no autorizadas y datos alterados, se debe realizar un seguimiento exhaustivo y generar procedimientos correctivos para evitar futuras recurrencias.
6) Buscar y reparar consecuencias provenientes de incidentes de seguridad de la información

ACCIONES DISCIPLINARIAS

La violación de esta política puede resultar en acciones disciplinarias que puede dar término a contrataciones de funcionarios; término de la relación laboral en el caso de contratistas o consultores; o suspensión o expulsión en el caso de un practicante. Adicionalmente los funcionarios están sujetos a perder el acceso a los privilegios, e iniciar un proceso civil y/o penal.

8.-POLÍTICA DE RESPALDO Y RESTAURACIÓN DE INFORMACIÓN

PROPÓSITO

El propósito de esta política de respaldo y restauración de información es establecer las reglas para el respaldo y restauración de la información electrónica de la lotería del Cauca.

AUDIENCIA

Las políticas de respaldo y restauración se aplican a todos los funcionarios internos y contratistas externos que son responsables de la manipulación, ejecución y propietarios de la información en la Lotería del Cauca.

POLÍTICAS

1) Establecer como medida de seguridad informática la necesidad de realizar copias de respaldo o backups periódicamente en los equipos de cómputo, servidor de archivos y servidores.
2) Determinar responsables (tanto de realizar las copias como de llevar a cabo la comprobación de la integridad de los datos almacenados) y responsabilidades.
3) Cada funcionario es responsable directo de la generación de los backups o copias de respaldo
4) El administrador del sistema es el responsable de realizar los respaldos de la información, restaurar la información y de mantener una versión reciente de los archivos más críticos de la empresa. Cada treinta días debe efectuarse

un respaldo completo del sistema y verificar que se haya realizado correctamente.

5) El proceso de respaldo y recuperación de la información de la empresa debe ser documentado y revisado periódicamente, con el fin de asegurar que son recuperables.
6) Ubicación final de la copias, los medios de almacenamiento debe realizarse en una zona alejada del cuarto de cableado en un lugar seguro y preferiblemente una copia en la nube. La información debe estar cifrada.
7) En caso de ser necesario el transportar información sensible o de carácter confidencial en una unidad portátil de almacenamiento (memoria USB Flash, disco duro, laptop, etcétera) esta debe ir cifrada.
8) Los distintos tipo de datos que se van a incluir en el backup deben estar clasificados de acuerdo con su importancia, etiquetados con nombre del servidor procedente, descripción de la información, fecha de emisión, clasificación de criticidad e información de propietario o responsable.
9) En el momento en que la información respaldada deje de ser útil a la organización, dicha información debe borrarse totalmente y de forma permanente.

ACCIONES DISCIPLINARIAS

La violación de esta política puede resultar en acciones disciplinarias que puede dar término a contrataciones de funcionarios; término de la relación laboral en el caso de contratistas o consultores; o suspensión o expulsión en el caso de un practicante. Adicionalmente los funcionarios están sujetos a perder el acceso a los privilegios, e iniciar un proceso civil y/o penal.

9.-POLÍTICA DE USO DE DISPOSITIVOS EXTRAÍBLES

PROPÓSITO

El propósito de la política de uso de dispositivos extraíbles es establecer las reglas para el buen manejo de los dispositivos de almacenamiento extraíbles y portables de la lotería del Cauca.

AUDIENCIA

La política de uso de dispositivos extraíbles se aplican a todos los funcionarios internos/externos y/o visitantes responsables de la manipulación, ejecución y propietarios de la información dentro la lotería del Cauca.

POLÍTICAS

1) El proceso de sistemas será el responsable de establecer las autorizaciones a usuarios para el uso de dispositivos de almacenamiento externo, como Pen Drives o Memorias USB, Discos portátiles, Unidades de Cd y DVD Externos, para el manejo y traslado de información o realización de copias de seguridad o Backups.
2) El responsable del proceso de sistemas debe de reportar el listado de los funcionarios con autorización de uso de este tipo de dispositivos, especificando clase, tipo y uso determinado.
3) Los usuarios que tengan asignados estos tipos de dispositivos serán responsable del buen uso de ellos.

4) Si algún área o dependencia por requerimientos muy específicos del tipo de aplicación o servicios de información tengan la necesidad de contar con un dispositivo de almacenamiento extraíble, deberá ser justificado y autorizado por el área de sistemas con la respectiva autorización de la alta dirección.
5) Todo funcionario de la lotería del Cauca deberá reportar al área de sistemas el uso de las memorias USB asignados para su trabajo, de carácter personal y responsabilizarse por el buen uso de ellas.

ACCIONES DISCIPLINARIAS

La violación de esta política puede resultar en acciones disciplinarias que puede dar término a contrataciones de funcionarios; término de la relación laboral en el caso de contratistas o consultores; o suspensión o expulsión en el caso de un practicante. Adicionalmente los funcionarios están sujetos a perder el acceso a los privilegios, e iniciar un proceso civil y/o penal

10.-POLÍTICA DE USO DEL INTERNET

PROPÓSITO

El propósito de esta política de uso de redes y acceso a internet es establecer las reglas para el uso efectivo, ético, moral y legal de los recursos de la red e internet de la empresa

AUDIENCIA

La política de uso de red y acceso a internet se aplican a todo el personal que labora en la lotería del Cauca.

POLÍTICAS

1) El servicio de internet es ofrecido para el personal que labora en la empresa, el uso de este recurso por personas ajenas a la misma queda terminantemente prohibida sin previa autorización.
2) El acceso a internet debe realizarse mediante servidores proxy, los cuales deben tener configuradas políticas de seguridad que generen restricción de acceso a lugares y/o puertos específicos que puedan causar daños a la empresa o representen una vulnerabilidad.
3) El acceso a la información en internet debe ser de carácter institucional, no puede tener contenido pornográfico o contenido lesivo contra la integridad de la empresa o una persona.
4) Las descargas deben ser controladas, el ancho de banda restringido y no es permitido el uso aplicaciones relacionadas con p2p y torrens.
5) Todo equipo de comunicación inalámbrica de be cumplir como mínimo con el estándar 802.11b.
6) Funcionarios distintos a los ligados al proceso de sistemas no pueden realizar instalaciones hardware o software.
7) Los usuarios no pueden extender o retransmitir los servicios de la red en cualquier forma.
8) Los usuarios o equipos informáticos que requieran conectividad a la red deben de ajustarse a las normas en esta política y siempre con autorización.
9) Todos los puntos de acceso inalámbrico deben de ser registrados y aprobados por el área de sistemas al igual que su instalación o personal

técnico autorizado. A estos equipos se le beben modificar las configuraciones de fabrica

10) El SSID debe ser configurado de forma que no muestra información de la empresa y estar oculto.
11) Ningún funcionario debe conectarse a la red sin una previa autorización del área de sistemas.
12) No se debe permitir ni fomentar el uso de la red inalámbrica para el transporte de información confidencial o critica de la empresa.
13) Cualquier quipo conectado a la red que represente un riesgo de seguridad para la red podrá ser desconectado sin previo aviso y la persona que posea el quipo será registrado y notificado.
14) El administrador del proceso de sistema es responsable y no limitarse a:

- ✓ Monitoreo el rendimiento y seguridad de todos los equipos de comunicación para prevenir accesos no autorizados y controlar de acceso a la web.
- ✓ Los recursos para las comunicaciones inalámbricas.
- ✓ Proveer asistencia, orientación y recomendaciones sobre el equipo de comunicaciones inalámbricas.
- ✓ Mantener un registro de todas las tarjetas de comunicación inalámbrica y puntos de acceso de la empresa.
- ✓ Planear, implementar y ejecutar programas de control de seguridad y acceso a la web.

ACCIONES DISCIPLINARIAS

La violación de esta política puede resultar en acciones disciplinarias que puede dar término a contrataciones de funcionarios; término de la relación laboral en el caso de contratistas o consultores; o suspensión o expulsión en el caso de un practicante.

Adicionalmente los funcionarios están sujetos a perder el acceso a los privilegios, e iniciar un proceso civil y/o penal.

11.-POLÍTICA DE LICENCIAMIENTO DE SOFTWARE

PROPÓSITO

El propósito de esta política de licenciamiento de software es establecer el marco regulatorio en donde se definen los procedimientos para instalación, manipulación y uso responsable de las herramientas de software licenciadas adquiridas por la lotería del Cauca.

AUDIENCIA

La política de licenciamiento de software aplica al Responsable del área de sistemas, Profesional Universitario Grado 01.

POLÍTICAS

1) Mantener bajo resguardo las licencias de uso del software de la empresa.
2) Llevar un control detallado las licencias en operación y los equipos en los cuales se encuentra en uso.
3) Planear y ejecutar la inspección de los equipos ofimáticos de la empresa en intervalos regulares.
4) Difundir a los usuarios las políticas de licenciamiento de software en busca de dar a conocer la normativa existente.
5) Analizar las necesidades y requerimientos de software de la empresa.

6) El registro documentado de las licencias debe contener:

- ✓ Nombre del software.
- ✓ Empresa desarrolladora.
- ✓ Versión.
- ✓ Fecha de adquisición.
- ✓ Fecha de vencimiento.
- ✓ Tipo de garantía.
- ✓ Tiempo de garantía.
- ✓ Contacto de soporte.

7) El soporte requerido para el software y aplicaciones web de uso corporativo debe ser exigido por el tiempo que se dará uso a la herramienta, de ser necesario debe ser actualizado de forma anual.
8) La contratación de soporte debe incluir la clacificación de los incidentes y los tiempos de respuesta por parte del proveedor.
9) El software adquirido por la Lotería del Cauca a modo de código fuente propio, debe realizar la inscripción a soporte lógico (software) en el Ministerio del interior y de justicia dirección nacional de derecho de autor UAE oficina de registro.

ACCIONES DISCIPLINARIAS

La violación de esta política puede resultar en acciones disciplinarias que puede dar término a contrataciones de funcionarios; término de la relación laboral en el caso de contratistas o consultores; o suspensión o expulsión en el caso de un practicante. Adicionalmente los funcionarios están sujetos a perder el acceso a los privilegios, e iniciar un proceso civil y/o penal.

12.-POLITICA DE CONEXIÓN REMOTA (TRABAJO EN CASA)

A partir del 20 de marzo de 2020, según Decreto 417 de 17 de marzo de 2020 de Presidencia de la República de Colombia, se declara el estado de Emergencia Económica, Social y Ecológica; debido al estado de Pandemia mundial COVID19.

Decreto 457 de 22 de marzo de 2020, Presidencia de la República, Ordena el asilamiento preventivo en todo el país.

Estrategia de la Lotería del Cauca: -Verificar los Decretos con fuerza de ley que se expidan por el Gobierno Nacional y que impacten el objeto misional de la Lotería del Cauca.

Estrategia de la Lotería del Cauca: - Autorizar por acto administrativo el trabajo en casa a todos los funcionarios y contratistas de la Lotería del Cauca.

PROPÓSITO

El propósito de esta política de uso de conexión remota, acceso a internet y a la información de cada computador asignado a cada uno de los funcionarios vinculados laboralmente a la Lotería del Cauca desde conexión remota desde casa, como objetivo de preservar la vida del personal que labora en la Lotería del Cauca y sus familias, cumplir las disposiciones expedidas por el Gobierno Nacional, con ello establecer las reglas para el uso efectivo, ético, moral y legal de los recursos de herramientas de conexión remota, red e internet de la empresa

AUDIENCIA

La política de uso de conexión remota, red y acceso a internet se aplican a todo el personal interno y externo que labora en la lotería del Cauca, y tiene a su cargo herramientas tecnológicas (computador) para su labor diaria.

POLÍTICAS

1) El servicio de internet es ofrecido para el personal que labora en la empresa, el uso de este recurso por personas ajenas a la misma queda terminantemente prohibida sin previa autorización.
2) El acceso a conexión remota se realizará mediante herramienta descargada en cada computador por los funcionarios del área de sistemas, con su respectiva clave.
3) El acceso a la información debe ser de carácter institucional, no puede tener contenido pornográfico o contenido lesivo contra la integridad de la empresa o una persona.
4) Las descargas deben ser controladas, el ancho de banda restringido y no es permitido el uso aplicaciones relacionadas con p2p.
5) Todo equipo de comunicación inalámbrica debe cumplir como mínimo con el estándar 802.11b.
6) Funcionarios distintos al proceso de sistemas no pueden realizar instalaciones hardware o software.
7) Los usuarios no pueden extender o retransmitir los servicios de la conexión en cualquier forma.
8) Los usuarios o equipos informáticos que requieran conectividad deben de ajustarse a las normas en esta política y siempre con autorización.

9) Cualquier equipo conectado a la red que represente un riesgo de seguridad para la red podrá ser desconectado sin previo aviso y la persona que posea el equipo será registrado y notificado.

10) El Responsable del área de sistemas del es responsable y no limitarse a:

- ✓ Monitoreo el rendimiento y seguridad de todos los equipos de comunicación para prevenir accesos no autorizados y controlar de acceso a la web.
- ✓ Proveer asistencia, orientación y recomendaciones sobre las conexiones remotas, videollamadas y reuniones en meet, zoom, etc
- ✓ Planear, implementar y ejecutar programas de control de seguridad y acceso a la web.

ACCIONES DISCIPLINARIAS

La violación de esta política puede resultar en acciones disciplinarias que puede dar término a contrataciones de funcionarios; término de la relación laboral en el caso de contratistas o consultores; o suspensión o expulsión en el caso de un practicante. Adicionalmente los funcionarios están sujetos a perder el acceso a los privilegios, e iniciar un proceso civil y/o penal.