PLAN DE POLITICAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

CORPORACION DE CULTURA Y TURISMO DE ARMENIA

MARZO 2019

ARMENIA QUINDIO.

Tabla de contenido

TABLA DE ILUSTRACIONES

INTRODUCION

En este documento se describe el uso y el modelo a seguir bajo las cuales se van a implementar la Política General y las Políticas de seguridad y privacidad de la información dentro del Corporación de Cultura y Turismo de armenia (CCTA), en las cuales se adoptaran las mejores prácticas planteadas por Mintic en su marco de referencia de la arquitectura empresarial y de TI de gobierno en línea ahora llamado también Gobierno Digital, en su modelos de seguridad y privacidad de la información, basándose y apoyándose en las normas y estándares de seguridad como lo son la norma iso 27001/2013.

Este va sujeto a la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI. En la Entidad el manual está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, veracidad, confiabilidad y disponibilidad de los activos de información y sus servicios, garantizando su buen uso y la privacidad de los datos.

Las políticas de seguridad y privacidad de la información descritas en este modelo, son parte fundamental para el buen uso y apropiación de buenas prácticas, para el sistema de gestión de seguridad de la información de la entidad y se convierten en un aliado del PETI para el buen funcionamiento e implementación de controles, procedimientos de estándares de seguridad. Además de ser aliados son parte de la familia de Gobierno en línea, la cual cuenta con sus procesos o etapas que son Tic para servicios, Tic para gobierno abierto, tic para Gestión y seguridad y privacidad de la información de la cual hace parte este manual. Estas políticas serán divulgadas formalmente a todos los funcionarios y se establecerá mecanismos de seguimiento y control, sobre el conocimiento y aplicación de las mismas.

JUSTIFICACION

Las organizaciones tanto públicas como privadas se han dado cuenta que, usando las tecnologías de la información, han logrado transformar, desarrollar y llevar a cabo sus planes estratégicos a niveles más avanzados. El Ministerio de Tecnologías de la Información y las Comunicaciones - Mintic a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; publica El Modelo de Seguridad y Privacidad de la Información (MSPI) en el cual se encuentra este manual incluido, y este se encuentra alineado con el Marco de Referencia de Arquitectura empresarial y TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.

La constante necesidad que tiene la CCTA de ajustarse rápidamente a los cambios que se dan en el ambiente tecnológico y de Gobierno digital, hace necesario que la administración tenga la información disponible, oportuna, confiable, veras y actualizada para poder tomar decisiones acertadas, esperando que la tecnología informática les ayude a tener una planificación más precisa de los recursos tecnológicos y del buen desempeño en la entidad a partir de la dirección estratégica en TI.

PROPOSITO

Elaborar de la política general y políticas de seguridad y privacidad de información para la corporación de cultura y turismo de armenia (CCTA), como parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea ítem seguridad y privacidad de la información, según lo establecido en el Decreto 1078 de 2015.

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Según la guía de política General de Mintic (MINTIC - GEL 2016).

La dirección en conjunto con la dirección TI, de la Corporación de Cultura y Turismo de Armenia, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad tanto estratégicas como de TI.

Para la CCTA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.

- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Corporación de Cultura y turismo de Armenia.
- Garantizar la continuidad del negocio frente a incidentes.
- LA CCTA ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Finalmente es de gran ayuda incluir la descripción general de otras políticas relevantes para el cumplimiento de los Objetivos planteados dentro del proyecto del SGSI ya que éstas son el apoyo sobre el cual se desarrolla; éstas deben ser descritas de forma sencilla, puntual y muy efectiva.

Dentro de las temáticas que se tocan en este punto se encuentran por ejemplo la gestión de activos, seguridad física y ambiental, control de accesos, etc. Para abordar este punto es necesario remitirse a la “Guía de políticas específicas de seguridad y privacidad de la información” y mencionar aquellas que la Entidad haya establecido como necesarias y primordiales. De esta forma se presenta el siguiente ejemplo:

A continuación, se establecen 10 principios de seguridad que soportan el SGSI de la Corporación de Cultura y Turismo de Armenia, las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.

• LA CCTA 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 (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

• LA CCTA 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.

• LA CCTA protegerá su información de las amenazas originadas por parte del personal.

• LA CCTA protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

• LA CCTA controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

• LA CCTA implementará control de acceso a la información, sistemas y recursos de red.

• LA CCTA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

• LA CCTA 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.

• LA CCTA garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

• LA CCTA garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

FASES DE IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Para que la Corporación de Cultura y Turismo de Armenia realice una correcta implementación de políticas de seguridad privacidad de la información, es necesario cumplir con una serie de fases y pasos a seguir que se sugieren en las guías establecidas por MINTIC bajo el marco de Referencia de la Arquitectura Ti y Empresarial, las cuales se muestran a continuación, estas tienen como objetivo que la entidad desarrolle, apruebe, implemente y socialice e interiorice las políticas para un uso efectivo y darse su cumplimiento por parte de todos los funcionarios, contratistas y/o terceros de la entidad.

Para la CCTA es importante contar con políticas de seguridad ya que son estas quienes guiaran el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad, así mismo las políticas permitirán que la entidad trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir la entidad a través de gobierno en Digital.

FASES:

1. **Desarrollo de las políticas**: En esta fase la Entidad debe responsabilizar las áreas para la creación de las políticas, estructurarlas, escribirlas, revisarlas y aprobarlas; por lo cual para llevar a buen término esta fase se requiere que se realicen actividades de verificación e investigación de los siguientes aspectos:

- Justificación de la creación de política: Debe identificarse el por qué la Entidad requiere la creación de la política de seguridad de información y determinar el control al cual hace referencia su implementación.

- Alcance: Debe determinarse el alcance, ¿A qué población, áreas, procesos o departamentos aplica la política?, ¿Quién debe cumplir la política?

- Roles y Responsabilidades: Se debe definir los responsables y los roles para la implementación, aplicación, seguimiento y autorizaciones de la política.

- Revisión de la política: Es la actividad mediante la cual la política una vez haya sido redactada pasa a un procedimiento de evaluación por parte de otros individuos o grupo de individuos que evalúen la aplicabilidad, la redacción y se realizan sugerencias sobre el desarrollo y creación de la misma.

- Aprobación de la Política: Se debe determinar al interior de la entidad la persona o rol de la alta dirección que tiene la competencia de formalizar las políticas de seguridad de la información mediante la firma y publicación de

  las mismas. Es importante que la Alta Gerencia de la Entidad muestre interés y apoyo en la implementación de dichas políticas.

2. **Cumplimiento:** Fase mediante la cual todas aquellas políticas escritas deben estar implementadas y relacionadas a los controles de seguridad de la Información, esto con el fin de que exista consistencia entre lo escrito en

las políticas versus los controles de seguridad implementados y documentados.

3. **Comunicación:** Fase mediante la cual se da a conocer las políticas a los funcionarios, contratistas y/o terceros de la Entidad. Esta fase es muy importante toda vez que del conocimiento del contenido de las políticas depende gran parte del cumplimiento de las mismas; esta fase de la implementación también permitirá obtener retroalimentación de la efectividad de las políticas, permitiendo así realizar excepciones, correcciones y ajustes pertinentes. Todos los funcionarios contratistas y/o terceros de la entidad debe conocer la existencia de las políticas, la obligatoriedad de su cumplimiento y la ubicación física de tal documento o documentos, para que sean consultados en el momento que se requieran.
4. **Monitoreo:** Es importante que las políticas sean monitoreadas para determinar la efectividad y cumplimiento de las mismas, deben crearse mecanismos ejemplo indicadores para verificar de forma periódica y con evidencias que la política funciona y si debe o no ajustarse.
5. **Mantenimiento:** Esta fase es la encargada de asegurar que la política se encuentra actualizada, integra y que contiene los ajustes necesarios y obtenidos de las retroalimentaciones.
6. **Retiro:** Fase mediante la cual se hace eliminación de una política de seguridad en cuanto esta ha cumplido su finalidad o la política ya no es necesaria en la Entidad. Esta es la última fase para completar el ciclo de vida de las políticas de seguridad y requiere que este retiro sea documentado con el objetivo de tener referencias y antecedentes sobre el tema.

POLITICAS ESPECÍFICAS RECOMENDADAS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

En este ítem se presentarán las Políticas de Seguridad y privacidad de la Información de acuerdo a la guía 2 Política general del modelo MSPI planteado por MINTIC bajo el marco de referencia de la arquitectura empresaria y TI que guiaran y se implementaran dentro de la entidad. A continuación, se agruparán las políticas con el objetivo de hacer una implementación transversal de Seguridad de la Información en la Corporación de Cultura y Turismo de Armenia (CCTA).

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Dentro de esta se identifican los actores involucrados que hacen parte del comité directivo de seguridad y privacidad de la información de la CCTA , a continuación se nombrara el Comité Institucional de Desarrollo Administrativo de la Corporación de Cultura y Turismo de Armenia, estará conformado por los siguientes miembros en los cuales se encuentran el Director General de la entidad o quien lo presida, líder del proceso de gestión financiera, líder del proceso de gestión administrativa, Jefe de la Oficina Asesora de Planeación quien actuará como secretario, Líder proceso gestión cultural, líder del proceso de la Banda sinfónica juvenil municipal, Jefe Oficina de Control Interno, quien tendrá voz pero sin voto. Estos mismos ya nombrados serán el comité de directivos de las políticas de seguridad de la información ya que este se encuentra dentro de mi PG en la sesión de Gobierno digital los cuales tienen como objetivo en cada comité revisar el avance de la implementación y el cumplimiento del manual de políticas de seguridad de la información, además la retroalimentación y el mejoramiento continuo de estas misma.

Ilustración 1 Comité de seguridad y privacidad de la información CCTA.
Fuente: autoría propia

GESTION DE ACTIVOS

En este apartado se describen políticas que hacen referencia a todas aquellas directrices mediante las cuales se indica a los funcionarios los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de Información.

Activos de Información

- La CCTA deberá actualizar el Inventario de los activos de información físicos cada seis meses, por el funcionario encargado en la entidad o quien haga sus veces, además que debe contar con placa de inventario que lo identifica como activo fijo de la entidad.
- Toda la información de la CCTA, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que dicte la Oficina de TI. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.
- La CCTA implementara las directrices para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.
- La CCTA tiene la custodia sobre todo dato, información y mensaje generado, procesado y contenido por sus sistemas de cómputo, así como también de todo aquello transmitido a través de su red de telecomunicaciones o cualquier otro medio de comunicación físico o electrónico y se reserva el derecho de conceder el acceso a la información.
- La CCTA deberá realizar la clasificación de la información, evaluando las tres características de la información en las cuales se basa la seguridad de la información: confidencialidad, integridad y disponibilidad.
- El inventario de los activos de información digitales de la entidad (software, bases de datos y archivos digitales), es responsabilidad de la Oficina TI.
- Se debe realizar devolución de los activos de información de la entidad cuando una persona queda fuera de la entidad ej.: cuando es despedido o

renuncia y debe de ser recibido por la Oficina TI o el encargado de esta de la entidad.

- La información física y digital de la CCTA tiene 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 conservación, se le debe dar el tratamiento de acuerdo a la disposición final definida por la entidad.
- Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias: verificar las áreas adyacentes a impresoras escáneres, fotocopiadoras para asegurarse que no quedaron documentos relacionados o adicionales; así mismo, recoger de las impresoras escáneres, fotocopiadoras, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada o mal intencionada.
- Tanto los funcionarios como el personal provisto por terceras partes deben asegurarse que, en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren 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.

Gestión de activos de Información.

Hardware.

- El equipo de cómputo será asignado de acuerdo al puesto o función laboral en su área de trabajo. Siendo el responsable de dicha asignación el Director del Área.
- Cada equipo está preparado con el Hardware y Software básico necesario para su funcionamiento, el usuario no deberá alterar el contenido físico y/o lógico del mismo incluyendo sus periféricos.

- En caso de presentar una falla física o lógica se deberá notificar al área encargada y en el caso de ser requerido enviar el equipo para su revisión y/o reparación de acuerdo al procedimiento establecido.
- En ningún caso el usuario intentará reparar el equipo o diagnosticarlo, únicamente informar de la posible falla.
- El usuario será el único responsable del equipo de cómputo.
- En ningún caso, el usuario tendrá cerca alimentos, bebidas u otros materiales que puedan derramarse sobre el equipo.
- Solo se utilizará el equipo para funciones de interés del área y de ninguna manera para asuntos personales.
- El personal asignado deberá comprobar sus conocimientos o experiencia en el manejo del equipo de cómputo y periféricos básicos.
- En caso de que el usuario no tenga conocimientos y/o experiencia, se notificará al área de sistemas para su correspondiente Capacitación.
- La adquisición de equipo será con cargo al presupuesto de cada área o de la secretaria general, las características técnicas serán proporcionadas por el área de sistemas.
- La solicitud del equipo de cómputo será responsabilidad del área interesada, bajo las características técnicas definidas por el área de sistemas e informando a las áreas relacionadas con la asignación de los recursos.
- Por ningún motivo se deberá violar la etiqueta de control ya que cualquier daño o cambio al hardware será responsabilidad de la persona a quien este resguardado.

Software

- Cada equipo contiene el software de acuerdo a las necesidades del área de trabajo, el cual siempre debe tener el respectivo licenciamiento.
- No deberá ser alterado.
- Por ningún motivo el usuario instalará software de promoción y/o entretenimiento.
- El software no puede ser utilizado por el usuario para realizar trabajos personales.
- El personal asignado deberá comprobar sus conocimientos o experiencia en el manejo de los programas básicos de operación de PC's.

Uso De Internet

- El uso de Internet está limitado por las políticas de seguridad del área de sistemas.

- Los Accesos a la red (Internet) serán solo de interés laboral y no personal. Se establecen horarios de uso a fin de no saturar el canal y poder hacer un buen uso del mismo.
- Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN, Yahoo, Skype, Net2phome y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias de la CCTA.
- Las páginas de consulta común por su contenido de interés general y de carácter laboral como: páginas de carácter institucional, se pueden consultar en cualquier momento dentro del horario laboral.
- De ninguna manera se podrá acceder a páginas de entretenimiento, redes sociales, pornografía o fuera del contexto laboral.
- El usuario no deberá descargar (o copiar) archivos de la red sin autorización del área de sistemas.
- El usuario no debe ejecutar las opciones de actualización de programas que eventualmente aparecen cuando se navega en Internet.
- La comunicación estará limitada por las políticas de seguridad del área de Sistemas.
- Solo se enviará y recibirá información de interés laboral.
- En ningún caso de recibir información en archivos adjuntos de dudosa procedencia o que no esté esperando, se notificará al área de sistemas, para analizar y evitar que ingresen virus al sistema.
- No se deberá enviar información de tipo estadístico, informativo o información relevante de las acciones de la Dirección, Área de trabajo o del Gobierno Municipal a ningún destino no autorizado.
- Para el desarrollo o modificaciones del sistema, el usuario deberá presentar su solicitud al área de sistemas para su evaluación.
- Se tienen correos institucionales dentro de la política de austeridad en el gasto público, se recomienda su uso para toda la comunicación interna y ahorrar tinta y papel.
- El direccionamiento y la configuración asignada a los equipos dentro de la LAN es de uso exclusivo del equipo asignado al funcionario por la oficina de sistemas. Cualquier modificación al respecto, está prohibida pues genera traumatismo en el esquema de seguridad de LAN.

Operaciones Básicas

- Para encender el sistema de cómputo verifique que el monitor, CPU, impresora y demás periféricos estén debidamente instalados entre si y conectados a la corriente eléctrica.
- Enseguida identifique los interruptores o botones de encendido y apagado presione o mueva según se requiera.
- Encienda la Impresora, regulador/no-break, monitor, y demás periféricos que tenga instalados dejando al final el CPU.
- Para apagar el sistema presione o mueva los interruptores según se requiera en el mismo orden antes mencionado (algunos equipos requieren que se mantenga presionado el botón unos segundos).
- Encender y apagar el Sistema: Al inicio y fin de las actividades, En caso de tormentas eléctricas, Si se presentan fallas eléctricas.

Imagen Institucional

- Todos los equipos podrán tener como imágenes predeterminadas aquellas que sean institucionales.
- En el exterior de todos los equipos se respetará la imagen física de empaque.
- Todos los accesorios de apoyo podrán tener plasmadas imágenes institucionales.
- Cada usuario es responsable del cuidado de su herramienta de trabajo. Por lo que se recomienda limpiar continuamente el equipo externamente.

Seguridad Personal

- Parpadee continuamente para evitar que las pupilas se sequen, especialmente si usa lentes de contacto.
- Cambie periódicamente la dirección de su mirada para descansar el nervio ocular.
- Realice constantemente ejercicios de visión periférica.
- Mantenga limpia la pantalla del monitor para facilitar la lectura y evitar reflejos.

- Regule la iluminación del área para evitar el reflejo de la luz sobre la pantalla.
- Emplee filtros que obscurecen el brillo de la pantalla y disminuyen la disipación de rayos ultravioleta (de vidrio o plástico en vez de maya, ya que éste tiende a recoger el polvo).
- Ajuste la brillantez de la pantalla.
- Ajuste la posición de la pantalla y las fuentes de iluminación (luz natural y eléctrica).
- Coloque el monitor y los documentos fuente de manera que ambos estén aproximadamente a la misma distancia de sus ojos.
- Remplace los monitores con mala resolución o parpadeo.
- Si utiliza lentes que sean con un marco completo para leer a una distancia de 50 a 60 centímetros.

CONTROL DE ACCESO

- En caso de que el funcionario tenga implementada una clave de acceso al equipo asignado, ésta tendrá que ser informada al personal de la oficina de Sistemas.
- Todos los equipos de la Corporación tienen contraseña de administrador para que los usuarios no realicen cambios sin autorización.
- Cada funcionario o contratista de la entidad que deba usar una contraseña y un ID para alguno de los sistemas de información de la entidad, debe de dirigirse a la oficina de TI y solicitar la asignación de esta.
- Cada usuario es responsable de su id y contraseña y es único e intransferible, en caso de que se acabe su vinculación con la entidad debe reportarlo a la oficina de TI para cancelar su usuario y verificar que todo esté en orden.

- Los funcionarios que usen llaves digitales en la Entidad deben ser responsables de cualquier trámite que se haga con esta además es personal e intransferible y no debe prestarse ni compartirse.
- Las contraseñas serán Establecidas por cada funcionario o contratista de la entidad y estas deben ser debidamente actualizadas. Con mínimo una mayúscula, un número y un carácter especial
- Ningún funcionario o contratista de la entidad, debe acceder a información de los servidores o bases de datos sin la debida autorización de la oficia TI.
- No se permite sacar o revelar información privada de la entidad a terceros.
- Cualquier documento físico que llegue o salga de la entidad debe ser solo recibido por la persona encargada de radicación y ella asignara a su funcionario correspondiente o realizara el envió de esta a el tercero.
- El área de sistemas auditará de manera periódica los equipos de cómputo y periféricos, así como el software instalado.
- Cualquier salida y/o entrada de información tendrá que ser bajo la responsabilidad del jefe inmediato.
- Solo los equipos portátiles de propiedad dela Corporación de Cultura y Turismo de Armenia podrán desplazarse con previa autorización del responsable de la dependencia y bajo la responsabilidad total del usuario.
- Todo servidor público es responsable de salvaguardar su información, y debe hacer copias de seguridad por lo menos una vez en el mes. Las copias deben ser debidamente rotuladas, y mantenerse en lugares seguros.
- Los interventores son responsables de verificar los medios magnéticos que reciben como producto o respaldo de objetos contractuales.
- Es responsabilidad de los propietarios de los activos de información, definir los perfiles de usuario y autorizar, conjuntamente con la oficina de TI, las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.

- Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.

NO REPUDIO

- Todo uso que se haga de los recursos informáticos de la entidad deben ser seguidos y auditados por el comité de políticas de seguridad de la información.
- Los funcionarios o contratistas de la entidad están en todo el derecho de realizar acciones con la información de la entidad siempre y cuando sean autorizados y en bien de la institución.
    - La política hará que por medio de la trazabilidad de las acciones se haga seguimiento a la creación, origen, recepción, entrega de información y otros.
    - La política debe incluir el periodo de retención o almacenamiento de las acciones realizadas por los usuarios, el cual deberá ser informado a los funcionarios, contratistas y/o terceros de la Entidad.
    - La política incluirá la realización de auditorías continuas, como procedimiento para asegurarse que las partes implicadas nieguen haber realizado una acción.
    - La política incluirá en los casos que aplique, que los servicios de intercambio electrónico de información son garantía de no repudio.

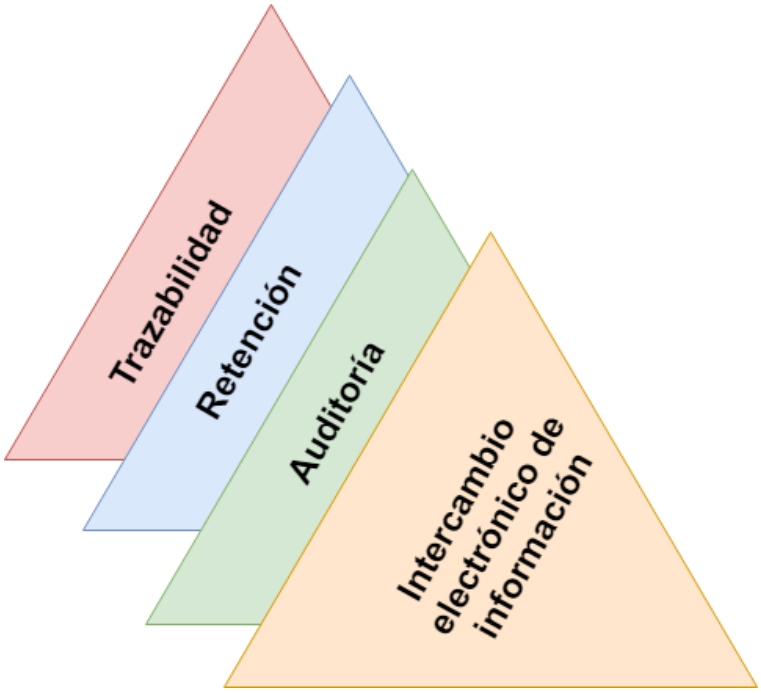

Ilustración 2 Aspectos no repudio
Fuente: autoría propia

PRIVACIDAD Y CONFIDENCIALIDAD

- La Corporación de Cultura y Turismo de Armenia se comprometerá con la privacidad y confiabilidad de la información suministrada tanto por usuarios, funcionarios, contratistas y/o terceros a manejar está bajo absoluta reserva y cumplir con lo establecido en los siguientes principios concertados por Mintic en la arquitectura GEL MSPI en su guía política general de la privacidad y seguridad de la información.

Ilustración 3Principios privacidad y confidencialidad
Fuente: autoría propia

- **Principio de la Legalidad:** El tratamiento de datos personales dentro de la CCTA debe estar sujeto a lo establecido en la normatividad vigente.
- **Principio de finalidad:** la CCTA debe Indicar la finalidad del tratamiento de datos personales, la cual debe ser informada al titular de estos.

- **Principio de libertad:** La CCTA solo realizara autoriza que el tratamiento sólo puede hacerse con el consentimiento previo, expreso e informado del titular de los datos.
- **Principio de veracidad o calidad:** La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- **Principio de transparencia:** La CCTA Garantizara al titular de los datos el derecho a obtener información que le concierna del encargado del tratamiento.
- **Principio de acceso y circulación restringida**: El tratamiento sólo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normatividad vigente.
- **Principio de seguridad**: La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento
- **Principio de confidencialidad:** Todas las personas que participen en el Tratamiento de Datos Personales deben garantizar la reserva de dicha información.

- La Corporación de Cultura y Turismo de armenia cumplirá con lo siguiente en cuanto a la privacidad y la confiabilidad de la información mediante los usuarios y funcionarios.
  - Conocer, actualizar y rectificar sus datos personales.
  - Solicitar la prueba de su autorización para el tratamiento de sus datos personales.
  - Ser informado respecto del uso que se les da a sus datos personales.
  - Revocar la autorización y/o solicitar la supresión de sus datos personales de las bases de datos o archivos cuando el titular lo

considere, siempre y cuando no se encuentren vigentes con el Banco los servicios o productos que dieron origen a dicha autorización.

- Presentar quejas ante la entidad administrativa encargada de la protección de los datos personales.

- Si la CCTA en algún momento va realizar uso de datos de una persona debe primero buscar la autorización con la persona solicitada en este caso para el tratamiento de sus datos e información.
- En la CCTA cualquier dato o información suministrada en los sistemas de información de la institución va estar bajo absoluta privacidad y confiabilidad, por el compromiso adquirido tanto de funcionarios, contratistas y/o terceros además del cumplimiento de este plan.
- La política de confidencialidad, debe contener un compromiso o acuerdo de confidencialidad, por medio del cual todo funcionario, contratista y/o tercero vinculado a la Entidad, deberá firmar un compromiso de no divulgar la información interna y externa que conozca de la Entidad, así como la relacionada con las funciones que desempeña en la misma. La firma del acuerdo implica que la información conocida por todo funcionario, contratista y/o tercero, bajo ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización.

INTEGRIDAD

La Corporación de Cultura y Turismo de Armenia está comprometida con el buen uso del manejo e integridad de la información suministrada y que haga parte de la institución sea de actores internos o externos te, mediante la cual debe ser cumplida por funcionarios, contratistas y/o terceros de la entidad.

De esta manera, toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente,

exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información. En el caso de vinculación contractual, el Compromiso de administración y manejo integro e integral de la información interna y externa hará parte de las cláusulas del respectivo contrato, bajo la denominación de Cláusula de integridad de la información.

DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN

Dentro del Plan Estratégico de Tecnologías de Información (PETI) que se está realizando dentro de la entidad , se establecerá el plan maestro o mapa de ruta el cual incluye los proyectos o planes de continuidad en las secciones de gestión de información, con el fin de asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y procesos misionales de la Entidad, ante el evento de un incidente de seguridad de la información.

La CCTA velara por el cumplimiento de los niveles de disponibilidad de servicios e información acordados con los clientes, proveedores y/o terceros como lo son usuarios entre otros como también se dejará plasmado en el dominio de servicios Tecnológicos en el PETI.

La CCTA Velara por el cumplimiento de los acuerdos de nivel de servicio realizados con terceros para la disponibilidad de información de estos.

Se debe cumplir con la Gestión de cambios que se realice en cuanto a servicios de información y pautas establecidas por el comité de políticas de seguridad de la información.

REGISTRO Y AUDITORÍA

En este apartado se establecerá que la CCTA velara por el mantenimiento de las evidencias de las actividades y acciones que afectan los activos de información.

- El área de control Interno de la entidad y el comité de políticas de seguridad de la información, deben participar acerca de la responsabilidad de llevar a cabo las auditorías periódicas a los sistemas y actividades relacionadas a la gestión de activos de información, así como la responsabilidad de dicha Oficina de informar los resultados de las auditorías.
- La oficina TI debe incluir el almacenamiento de los registros de las copias de seguridad en la base de datos correspondiente y el correcto funcionamiento de las mismas. Los registros de auditoría deben incluir toda la información registro y monitoreo de eventos de seguridad.
- La auditoría debe velar porque las mismas sean realizadas acorde a la normatividad y requerimientos legales aplicables a la naturaleza de la Entidad.
- La CCTA deberá garantizar la evaluación de los controles, la eficiencia de los sistemas, el cumplimiento de las políticas y procedimientos de la Entidad; así como recomendar las deficiencias detectadas.
- Se determinará la revisión periódica de los niveles de riesgos a los cuales está expuesta la Entidad mediante el plan de riesgos de la seguridad y privacidad de la información, lo cual se logra a través de, Auditorías periódicas alineadas a los objetivos estratégicos y gestión de procesos de la entidad que se deben realizar cada seis meses como mínimo.

Ilustración 4 registro y auditorias
Fuente: autoría propia

En la anterior figura se ilustra la forma en cómo funciona o las bases para realizar las políticas que hacen referencia al apartado de registro y auditoria. La cual consta de Responsabilidad, almacenamiento de datos o registros, normatividad, garantías para el cumplimiento de las mismas y la periocidad.

GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

En este espacio se hablará de la gestión de incidentes y su ruta a tomar en caso de, este también se encontrará plasmado en el Plan Estratégico de Tecnologías de Información de la entidad que actualmente en su Dominio de servicios tecnológicos.

- Si ocurre cualquier incidente con los activos de información o seguridad de la misma debe comunicarse inmediatamente a la oficina TI de la entidad puede hacerse de forma manual o electrónica.
- El único encargado de solucionar o saber qué hacer en el caso de estos incidentes es la oficina TI de la entidad ningún funcionario o contratista debe solucionarlos.
- Se debe realizar un documento de gestión de reportes de incidentes para un inventario y una documentación clara de lo que ha pasado y la manera en se ha solucionado.
- La oficina TI será la encargada de comunicar la Gestión de Incidentes al Comité de políticas de seguridad.

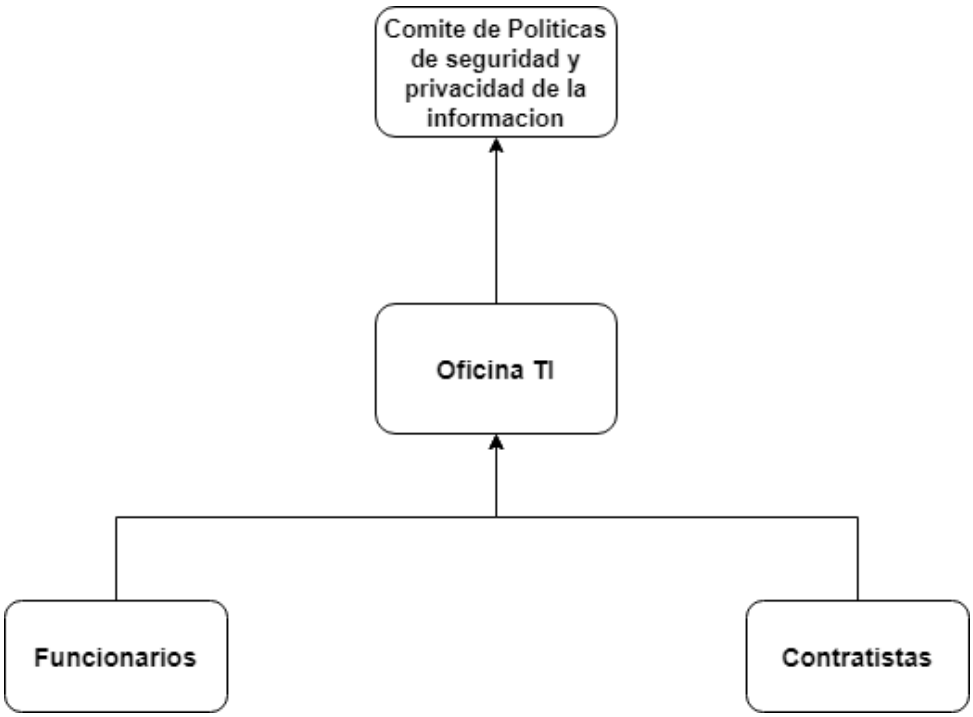

Ilustración 5 estructura de incidentes CCTA
Fuente: autoría propia

CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN.

Esta área se centra en la formación del personal en temas relacionados con la seguridad de la información, cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano.

- Todos los funcionarios y contratistas de la CCTA deben tener presente este plan de políticas de seguridad y privacidad de la información.
- Realizar un espacio de capacitación para compartir la información aquí establecida con todos los funcionarios de la CCTA en el cual se socialicen las políticas aquí establecidas.
- Revisión periódica de resultados de capacitaciones para mejoramiento de los procesos.
- La comunicación se realizará por parte del comité de políticas de seguridad y privacidad de la información de la entidad.
- Los funcionarios y contratistas de la entidad deben cumplir con lo ya establecido dentro de este plan una vez sea aprobado, socializado e implementado.
- Actualizar el plan mínimo cada seis meses y realizar su respectiva comunicación de la actualización con los funcionarios y terceros.

CONCLUSIONES

- La formulación de políticas es un elemento imprescindible cuando se pretende gestionar la seguridad de la información en una empresa y sus actividades que conllevan a las mejores prácticas.
- Las políticas de seguridad y privacidad de la información descritas en este modelo, son parte fundamental para el buen uso y apropiación de buenas prácticas, para el sistema de gestión de seguridad de la información de la entidad.
- El buen uso de este plan dentro de la entidad conllevara a una buena gestión y evaluación para esta además de cumplir con los estándares establecidos por Mintic en su estructura GEL ítem Seguridad y privacidad de la información.
- Las políticas de seguridad y privacidad se realizan con base a las necesidades de la entidad, las cuales se identifican en cada ámbito para así dar cumplimiento a estas mismas con mucho profesionalismo.
- Las políticas establecidas aquí son concisas, fácil de leer y comprender, flexibles y fáciles de hacer cumplir para todos aquellos dentro del alcance sin excepción. Son cortas, y enmarcan los principios que guían las actividades dentro de la entidad.

BIBLIOGRAFIA

MINTIC - GEL. 2016. “Política General de Seguridad y Privacidad de La Información.” (2). https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf.