PERSONERIA MUNICIPAL DE EL COPEY CESAR

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

RAFAEL FONTALVO CORREA PERSONERO MUNICIPAL

ENERO DE 2023

OBJETIVO

Dar a conocer las Políticas de Seguridad de la Información y Estándares de Seguridad Informática, que deben aplicar y acatar todos y cada uno de los empleados, contratistas y terceros de la Personeria Municipal de El Copey Cesar entendiendo como premisa que la responsabilidad por la seguridad de la información no depende únicamente del Gerente, sino que es una responsabilidad de cada empleado, contratista y tercero activo de la Empresa.

Establecer Políticas de seguridad de la Información alineadas a la normatividad Vigente en Seguridad de la Información y a los estándares actuales, con el fin de velar, cuidar y resguardar la confidencialidad, la integridad y asegurar la disponibilidad de la información.

ALCANCE

Este documento define las Políticas de gestión de riesgo y Estándares de Seguridad de la Información que deben ser cumplidos por:

- Todas las Áreas de la Personeria Municipal de El Copey Cesar.” Por su condición de gestora, procesadora y protectora de todo tipo de información soportada en cualquier medio físico impreso o electrónico.
- Todos los empleados y contratistas de la Personeria Municipal de El Copey Cesar Que accedan a información sensible de la Empresa o de sus Usuarios, dentro del marco de los servicios prestados.

NORMATIVIDAD

- NTC-ISO-IEC-27001: Tecnología de la información. técnicas de seguridad. Sistemas de gestión de la seguridad de la información. requisitos.
- NTC-ISO-IEC-27002: Tecnología de Información. técnicas de seguridad. Código de prácticas para controles de seguridad de la información.

- MSPI: MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN del Ministerio de Tecnologías de la Información y las Comunicaciones – Min TIC.
- Ley 1581 de 2012 Ley de Tratamiento de Datos Personales.
- Decreto 1377 de 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

PRINCIPIOS

Principio para el tratamiento de datos personales: Para el cumplimiento de los requerimientos mínimos de seguridad y Calidad de la información que se maneja a través de canales y medios de distribución de productos y servicios para clientes y usuarios, se deberán tener en cuenta los siguientes Principios rectores.

Principio de Confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

Principio de veracidad o calidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

Principio de legalidad en materia de Tratamiento de datos: El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.

Principio de finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

Principio de transparencia: En el Tratamiento debe garantizarse el derecho del Titular a obtener del responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la Ley.

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente.

Principio de seguridad: La información sujeta a Tratamiento por el responsable o Encargado de este proceso a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

POLÍTICA GENERAL SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Personeria Municipal de El Copey Cesar, adopta esta política a fin de garantizar el desarrollo normal de sus actividades y la prestación de sus servicios objeto del negocio, y se compromete de manera expresa a resguardar, proteger y a reducir todo riesgo que se pueda presentar con las fuentes de información manejadas en nuestra Entidad, de manera que se mantendrá una conciencia por promover la cooperación de cada persona que hace parte de la operación, así como también

estaremos al tanto de nuevas herramientas y tendencias administrativas que nos faciliten el control, apuntando a la eficiencia y eficacia de los procesos basados en la Normatividad Vigente.

- Utilizar de forma leal y responsable los equipos, periféricos y suministros asignados por la Entidad para su diaria labor.
- Los recursos informáticos suministrados para ejecutar sus labores diarias son para uso exclusivo de la labor contratada, y nunca para uso personal.
- No se puede instalar software gratis o de libre distribución en los equipos de cómputo de la Personeria Municipal de El Copey Cesar.
- No se debe realizar cualquier actividad que tenga la intención de introducir programas maliciosos (tales como virus, gusanos, troyanos) que rastreen, exploten la vulnerabilidad en los equipos o que pueden comprometer los servicios informáticos, de la red de la Entidad.
- Las contraseñas y Usuarios son de uso personal e intransferible, por tal razón no se deben compartir, prestar, divulgar por ningún motivo; por el uso indebido se aplicarán las sanciones contempladas en el procedimiento de Incidentes de seguridad de la información.
- Todos los funcionarios que tengan acceso a un equipo de cómputo y que se les haya asignado Usuarios de Ingreso, deben cambiar la contraseña al momento de realizar el primer ingreso.
- Todos los funcionarios que tengan acceso a un equipo de cómputo y que se les haya asignado Usuarios de Ingreso, deben comprometerse a tener contraseñas de mínimo 14 caracteres, alfas numéricas y con caracteres especiales, sin que contengan sus nombres o apellidos, o datos que sean de fácil acceso.
- Las contraseñas deben cambiarse con una periodicidad de 60 días y las últimas dos (2) contraseñas no pueden ser repetidas.
- El usuario no debe tener en su escritorio anotaciones de sus claves.
- Los empleados que tengan acceso a correo corporativo se comprometen a utilizarlo únicamente con fines laborales y nunca con fines personales.
- Los empleados que tengan acceso a correo corporativo se comprometen a NO enviar por correo información confidencial o que viole la ley 1581 de Protección de Datos.
- Los empleados que tengan acceso a correo corporativo se comprometen a NO enviar por correo información que contenga datos personales de titulares.
- Los empleados que tengan acceso a correo corporativo se comprometen a NO abrir correos de dudosa recepción, sino que serán eliminados de manera inmediata.
- Ningún funcionario debe manipular las cámaras de Video.

- En el momento que el usuario se ausente de su escritorio así sea por un espacio muy corto de tiempo por seguridad debe bloquear el equipo con la utilización simultanea de las teclas Windows + la tecla L.
- Cada uno de los funcionarios de la Personeria Municipal de El Copey Cesar." está en la obligación de poner en conocimiento de las directivas cualquier incidencia que atente contra el uso de la tecnología o cualquier otro aspecto de la misma
- En el evento de que un funcionario se retire de la "Personeria Municipal de El Copey Cesar " debe informar a la Gerencia quien debe dar a conocer de inmediato al área de sistemas este evento a fin de suspender sus claves, cuenta de correo, y todos los accesos a los sistemas y a las instalaciones.
- Los funcionarios no pueden tener acceso algunos sitios de Internet, a menos que necesiten páginas especiales, las cuales serán autorizadas por el área de Sistemas y se dará únicamente permiso a ellas si es necesario para el desarrollo de sus labores.
- Los usuarios no deben utilizar los equipos para visualizar o descargar pornografía.
- Los equipos no pueden ser utilizados para que el lucro personal de los usuarios, ni para realizar trabajos personales o trabajos de la universidad.
- Los Usuarios no pueden almacenar información en los discos locales.
- El no acatamiento de las normas establecidas en el presente documento, constituye una falta grave y en consecuencia acarreara sanciones disciplinarias contempladas en el Procedimiento de Incidentes de Seguridad.

RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN

- Todos los manuales, políticas y procedimientos de la Personeria Municipal de El Copey Cesar.", deben contar con la aprobación del personero.
- Monitorear los riesgos que afectan a los recursos de la información y las posibles amenazas, sean internas o externas.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes, relativos a la seguridad, que se produzcan en el tiempo de operación y fuera de la Entidad.
- Aprobar las iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada funcionario.
- Acordar y aprobar metodologías dentro de las buenas prácticas y estándares establecidos.
- Promover la difusión y apoyo a la seguridad de la información dentro de la Entidad.
- Mantener los planes de Continuidad de Toda la Operación.

POLÍTICA DE CONTROL DE CAMBIOS

- El comité de seguridad de la Información, es el responsable de revisar y aprobar cualquier cambio que se aplique al sistema de seguridad de la información de la Personeria Municipal de El Copey Cesar ,es decir, políticas, manuales, procesos, controles.
- Se responsabilizará del cambio el jefe del área que solicite el control.
- Se diligencia solicitud de cambio en el Formato correspondiente (Formato Solicitud y Control de Cambios).
- Se debe asignar al área encargada para su estudio previo.
- Si el cambio afecta la base de datos se debe evaluar la factibilidad teniendo en cuenta la comunicación, solución técnica, económica y los posibles riesgos.
- Una vez aprobado el cambio y con base en la planeación realizada, se prepara el cambio y el área de tecnología toma los controles necesarios para que no exista perdida de la información.
- El responsable del cambio comunicará verbalmente los detalles de los cambios que afectan a los usuarios con el fin de que estos estén enterados.

POLÍTICA DE ESCRITORIO LIMPIO

- Todo empleado debe conocer la importancia de tener su escritorio limpio, y la relación que tiene con la seguridad de la información de la Entidad.
- No se permite tener en los escritorios comida, ni bebidas diferentes a agua.
- Los empleados deben mantener el orden y la estética en su puesto de trabajo.
- Se mantendrá el aseo del lugar, y se mantendrán los escritorios y equipos ofimáticos libres de polvo y suciedad.
- Si el empleado se levanta de su puesto deberá dejar su pantalla bloqueada con la tecla Windows + L.
- Si algún empleado incurre en alguna falta a la política, esta será documentada como incidencia (Ver Procedimiento de Incidentes de la Seguridad de la Información) y se aplicará la sanción que aplique para la falta.

POLÍTICA DE INCIDENTES DE SEGURIDAD

- Se llamará Incidente de Seguridad todo uso indebido o intencional que vulnere la seguridad de la información y sus principios como la Confidencialidad, la integridad y la disponibilidad de la Información y donde se haya materializado un Riesgo.
- Todo el personal de la Personeria Municipal De El Copey Cesar , que tengan acceso a redes, aplicativos, programas, bases de datos y todo cualquier tipo de información que se encuentre en la Entidad debe adoptar y dar cumplimiento a esta política.
- El comité de Seguridad de la Información, debe evaluar los riesgos de Incidentes de seguridad y Clasificar según su Impacto y Urgencia.
- En la Personeria Municipal De El Copey Cesar. Se debe propender por minimizar el daño que un incidente podría causar en un momento específico de confusión.
- En la Personeria Municipal De El Copey Cesar ."se Establecerán y comunicarán las posibles consecuencias que puede generar un incidente a la Entidad. 9.15 Cualquier funcionario de la Empresa, puede denunciar un incidente de seguridad
- Los Incidentes de Seguridad deben ser Notificados a la persona que cometió el Incidente.
- A todos los incidentes de seguridad se les debe dar un tratamiento a fin de mitigar los Incidentes.
- Se informará a los funcionarios los procedimientos para Notificar un Incidente de Seguridad.

POLÍTICA DE SEGURIDAD FÍSICA

- La Personeria Municipal De El Copey Cesar, Tomará las medidas necesarias para proteger físicamente los recursos y la información de la organización, con los cuales los empleados interactúan, en general los activos de información, activos de software y activos físicos.
- La política aplica para todos los recursos; incluyen el personal, el sitio donde ellos laboran, los datos, equipos y los medios con los cuales los empleados interactúan, en general los activos.

- Toda área o equipo informático, debe cumplir con políticas de seguridad y procedimientos de seguridad física, con el fin de evitar el acceso por personas no autorizadas, daño e interferencia a los recursos e infraestructura de información.
- Se debe contar con pólizas al interior de la Empresa que cubran por lo menos hurto, y eventos de origen natural.
- Se deben consideran áreas seguras todos los sitios donde se encuentre sistemas de procesamiento informático, de almacenamiento, o de acceso a la información confidencial.
- El centro de cómputo siempre debe permanecer cerrado
- En caso de pérdida de llaves se debe garantizar el cambio de guardas de manera inmediata por parte del área administrativa de la Entidad.
- Se debe contar con extinguidores especiales para centros de cómputo
- Deben estar demarcadas las salidas de Emergencia en las zonas comunes.
- Se tienen extintores de incendios debidamente probados, y con capacidad de detener fuego generado por equipo eléctrico, papel o químicos especiales. o Explosivos.
- Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.
- No se puede tomar ningún tipo de bebidas o consumir alimento en el puesto de trabajo.
- Las conexiones de potencia deben tener su respectivo polo a tierra.
- La UPS debe garantizar el suficiente tiempo para realizar las funciones de respaldo en servidores y aplicaciones mínimo 15 minutos, para evitar cortos, daños en los sistemas de cómputo.
- Se deberán realizar mantenimientos sobre los equipos y debe ser realizados únicamente por personal autorizado.
- En los equipos donde se encuentre almacenada información esta debe ser destruida a través de actas de borrado y aplicativos de borrado, de realizar movimientos de los equipos fuera de la operación.
- Se prohíbe dejar en la impresora cualquier tipo de hojas con información sea confidencial o no.

POLÍTICA DE ASEGURAMIENTO DE LA INFRAESTRUCTURA

- La Personeria Municipal De El Copey Cesar, se compromete a asegurar los sistemas operativos y equipos pertenecientes a la infraestructura tecnológica de la Empresa, con el fin de elevar su nivel de seguridad, utilizando las mejores prácticas.
- Esta política Aplica para los Sistemas Operativos, Servidores, Equipos de Cómputo, Bases de Datos, Firewalls, Swiches, Routers, Telefonía.
- Se realizará la actualización de la matriz a fin de tener definido el control de las amenazas. (Matriz de Riesgos de Activos).

POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

- Toda la información, independientemente del medio en el que se encuentre (magnético, papel, etc.) debe estar clasificada en una de las siguientes categorías: Publica, Reservada de Uso Interno, Reservada confidencial, o Reservada Secreta.
- Se implementará los controles necesarios, a fin de proteger la Integridad, confidencialidad y disponibilidad de la Información
- Todos los funcionarios deben adoptar el procedimiento de clasificación de la información, para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado, y eliminación.
- La información que se encuentre en físico debe ser protegida a través de controles de acceso físico y las condiciones adecuadas de almacenamiento.

POLÍTICA DE CONTINUIDAD

- Esto implica que el Plan de Continuidad de la Entidad, contemplará todas las medidas preventivas y de recuperación para cuando se presente una contingencia que pueda afectar el desarrollo normal del trabajo y funcionalidad del negocio.
- La Personeria Municipal De El Copey Cesar ." dará a conocer a los empleados de la Entidad, el proceso para ejecutar el plan de continuidad en caso de que se presente.
- Se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos.
- Se deben tener contemplado en el Plan de Continuidad, los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.

POLÍTICA DE GESTIÓN DE USUARIOS Y CONTRASEÑAS

- Se debe evitar el acceso de usuarios no autorizados.
- Para el registro y cancelación de usuarios la Entidad debe definir y establecer un procedimiento de registro y desactivación de usuarios.
- Inmediatamente culmina el proceso de contratación, se debe solicitar por escrito los usuarios y accesos que se requieran para ejecutar su labor.
- En el momento de Ingresar la clave por primera vez esta debe solicitar cambio de manera automática.
- El funcionario en el momento de crear la nueva contraseña debe tener en cuenta que esta debe tener como mínimo 14 caracteres representados en números, letras mayúsculas y minúsculas y caracteres especiales como puntos, comas, punto y coma y dos puntos, y nunca debe contener el nombre y el apellido del usuario.
- Los usuarios y contraseñas son de uso personal y privado, no pueden ser compartidos con ningún otro empleado.
- No pueden existir usuarios genéricos o compartidos entre los usuarios.
- Se prohíbe prestar y divulgar los usuarios y contraseñas.
- En caso de presentar violación a esta política en materia de contraseñas, se aplicarán las sanciones de acuerdo a lo establecido en el procedimiento de Incidentes de Seguridad.
- Todos los funcionarios de la Empresa deben estar informados de los controles que deben seguir, según la política de control de acceso establecida, a los diferentes sistemas de información y activos con los que interactúan.
- La asignación de contraseñas debe estar controlada mediante un proceso de gestión formal por parte del departamento de Sistemas.
- En caso de que un funcionario tenga acceso a Bases de Datos en Hojas de Cálculo o Word, u otras, están deben encontrarse con contraseña de seguridad de mínimo de 14 caracteres y no puede ser genérica, ni compartida con otros usuarios.
- Se deben utilizar procedimiento o custodia de las claves o contraseñas en un sitio seguro.

POLÍTICA DE COPIAS DE SEGURIDAD

- La ubicación y Protección de Copias de Seguridad deberá ser ubicado y protegida de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.

- Se ubicarán en un sitio donde se minimice el acceso innecesario.
- Se Adoptarán controles adecuados para minimizar el riesgo de amenazas potenciales, por Robo o hurto, Incendio, Explosivos, Humo, Inundaciones o filtraciones de agua.
- Se Revisarán regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información. Esta revisión debería realizarse con una periodicidad no mayor a seis meses.

POLÍTICA DE ACCESOS REMOTOS

- La Personeria Municipal de El Copey, Cesar, debe asegurar que los funcionarios no realicen actos ilícitos o violen las políticas de la Entidad implementando una política general para acceder a los aplicativos.
- El acceso a los aplicativos o programas desde puntos remotos, independiente de la clasificación jerárquica, no se encuentran habilitados para ningún funcionario de la Entidad.

PROTOCOLOS DE ACCESO A LA INFORMACIÓN Y ACTIVOS.

- Deben existir protocolos de instalación, configuración, parametrización, gestión y soporte, de usuarios, roles y perfiles, para todos los sistemas de información existentes en la organización.
- Deben aplicarse políticas de gestión y control propias de los Sistemas de Información existentes.
- La instalación, configuración y parametrización de todos los sistemas de información de la Entidad debe ser responsabilidad del Ingeniero de Soporte designado.
- Los datos, bases de datos, programas, herramientas y sistemas de información de la Entidad deben ser modificados únicamente por personal autorizado de acuerdo con los procedimientos establecidos, al igual que el acceso a la información debe restringirse únicamente a personal autorizado por la Entidad.
- Se debe contar con un procedimiento que permita establecer los accesos y roles que tendrá cada funcionario en la Empresa, y los permisos que se den a cada rol.

POLÍTICA DE TELETRABAJO

- La Entidad brinda los lineamientos de seguridad digital para la protección de la información a la que se tiene acceso, se procesa o almacena en lugares en los que se realiza teletrabajos, y se hace uso de los recursos tecnológicos y activos de información autorizados por la Entidad para el desarrollo de las actividades de Teletrabajo, para lo cual se establecen las siguientes directrices:
- Toda información gestionada por la Entidad, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales con esta.
- La Entidad establece los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de los servidores públicos y contratistas de la entidad, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.
- La Entidad establece el proceso de implementación de teletrabajo, de acuerdo con la normativa y los lineamientos exigidos, con el fin de proteger la información.
- La Entidad revisa la seguridad física y del entorno del sitio donde se va a teletrabajar, con el fin de proteger la confidencialidad, integridad y disponibilidad.
- Al utilizar el dispositivo móvil en lugares públicos se recomienda mantenerlo siempre vigilado, utilizar guaya de seguridad y en caso de robo o pérdida del equipo notificar a los jefes de las áreas responsables para la realización del debido proceso.
- En los lugares que se realiza teletrabajo se debe aplicar las mismas políticas de uso de los activos de información, aplicación de contraseñas, bloqueo de sesión y demás que se relacionen, y en caso sospechar de un evento o incidente de seguridad, informar inmediatamente al área responsable.

POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS

- La Entidad establece directrices para asegurarse que los colaborares y contratistas tengan conocimiento sobre los derechos, deberes y responsabilidades en relación a la seguridad de la información, para lo cual se establecen las siguientes directrices:
- El área que realice la contratación de personal en la Entidad debe realizar las verificaciones de los antecedentes (procuraduría, contraloría, policía) de los candidatos al cargo, la

formación académica, experiencia y demás información que se requiera, de acuerdo a las leyes, reglamentos de la Entidad y ética pertinente.

- Todo servidor público y contratista debe recibir inducción y procesos periódicos de sensibilización en seguridad y privacidad de la información en la Entidad.
- La Entidad establece directrices para asegurar que los servidores públicos y contratistas tengan conocimiento sobre los derechos, deberes y responsabilidades en relación a la seguridad y privacidad de la información.
- Los acuerdos contractuales entre la Entidad y los servidores públicos o contratistas deben especificar el cumplimiento a los lineamientos de seguridad y privacidad de la información establecidos en la Entidad.
- El proceso de Talento Humano y el proceso de contratación cuando gestionan las actividades de desvinculación, licencias, vacaciones o cambio de labores de los servidores públicos y contratistas debe llevar a cabo los procedimientos y ejecutar los controles establecidos para tal fin, así mismo, los directores, jefes, supervisores de contrato o líderes deben informar la desvinculación o cambio de labores de acuerdo con los procedimientos, está información debe ser entregada oportunamente al proceso de TI.
- La Entidad debe incorporar los roles y responsabilidades en seguridad y privacidad de la información dentro de las funciones y obligaciones contractuales de los Colaboradores y Terceros.
- El incumplimiento o la violación de las políticas de seguridad de la información de la Entidad, por parte de los Colaboradores o Terceros, se les aplicará lo establecido en el proceso de investigaciones disciplinarias.

TOMA DE CONCIENCIA

Brindar lineamientos para que los servidores públicos, contratistas y proveedores de la Entidad reciban la educación y formación en toma de conciencia adecuada, y actualizaciones sobre las políticas y procedimientos.

Le proceso de Gestión de Talento Humano y el supervisor del contrato, deberán velar por que los servidores públicos, contratistas y proveedores de la Entidad, que desempeñen funciones en el mismo reciban entrenamiento y actualización periódica en materia de Seguridad de la Información.

Será responsabilidad de Recursos Humanos, incorporar la aplicación de las políticas de seguridad de la información en su plan de capacitación institucional, y velar por la correcta inducción de los funcionarios nuevos en materia de seguridad de la información.

COMUNICACIÓN

La Entidad deberá establecer los canales accesibles para la comunicación permanente de todas las políticas, procedimientos u otros documentos que hagan parte del Modelo de Seguridad y Privacidad de la Información (MSPI), algunos canales accesibles y formales para la comunicación son:

Correo Electrónico, Documentos Impresos y capacitaciones.

El presente Plan de Seguridad y Privacidad de la Información, será comunicado a todas las partes interesadas de la Entidad, a través de medios tecnológicos o físicos de ser necesario.

SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

La Entidad, debe asegurar que la seguridad y privacidad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales, para lo cual se establecen las siguientes directrices.

- Seguimiento de tareas, actividades o acciones asignadas en reuniones de comités donde se traten los temas de seguridad y privacidad de la información.
- Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y demás normas de seguridad y privacidad de la información.
- Realizar los cambios en las cuestiones internas y externas que sean pertinentes al MSPI.
- Analizar propuestas o mejoras al MSPI por parte de los servidores públicos y contratistas.
- Estado de acciones correctivas y de mejora (se evalúa la eficacia de las acciones), para Seguridad y privacidad de la Información sólo aplica las acciones correctivas y de mejora.
- Gestionar obtener la realimentación de las partes interesadas, respecto a la implementación de seguridad y privacidad de la información.
- Gestionar, analizar y documentar los resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos.

- Identificar las vulnerabilidades y amenazas no tratadas adecuadamente en la valoración previa de los riesgos.
- Revisión y actualización anual en caso que aplique de la política general, la revisión de las políticas específicas de seguridad, de objetivos de Seguridad de la Información (su contenido y cumplimiento en los diferentes procesos) por medio de planes de acción.

REVISIÓN PLAN DE SEGURIDAD DE LA INFORMACIÓN

La Alta dirección debe revisar el Plan de Seguridad y Privacidad de la Información (MSPI) de la Entidad, a intervalos planificados, ya que se tiene que asegurar la idoneidad, la adecuación, la eficiencia y la alineación continuas con los objetivos estratégicos de la Entidad, la revisión por la dirección tiene que planificarse y realizarse una vez al año el análisis de los resultados de la Evaluación y Desempeño.

RAFAEL FONTALVO CORREA

PERSONERO MUNICIPAL