MANUAL DE POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SECRETARÍA DE EDUCACIÓN Y CULTURA DEL TOLIMA

DICIEMBRE DE 2021

ELABORÓ	REVISÓ	APROBÓ
Macroproceso g. Gestión de la Información	LYDA GICELA GARZON AREVALO	Comité Institucional de Gestión y Desempeño
Fecha: 02-12-2021	Fecha: 02-12-2021	Fecha:

INDICE

1. Objetivo

Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la Entidad.

2. Alcance

Estas políticas y responsabilidades aplican para todos los funcionarios, proveedores y contratistas de la Secretaría de Educación y Cultura del Tolima.

Las políticas complementarias están enmarcadas en los siguientes capítulos:

1. Seguridad Recursos Humanos
2. Uso Aceptable Activos Información
3. Clasificación y Manejo Información
4. Política Control de Acceso
5. Seguridad física y del entorno
6. Seguridad de las operaciones de gestión tecnológica
7. Seguridad de las comunicaciones
8. Adquisición, Desarrollo Y Mantenimiento De Sistemas
9. Relaciones con los proveedores
10. Gestión de Incidentes de seguridad y privacidad de la información
11. Gestión de continuidad del negocio.
12. Usuarios Finales
13. Cumplimiento

2.1. Política Seguridad Recursos Humanos

Objetivo:

Concientizar e informar de forma continua a los funcionarios y contratistas sobre las políticas que afectan el desarrollo de sus funciones y de sus responsabilidades en materia de seguridad y privacidad de la información.

Políticas:

Antes de asumir el cargo

- Asegurar que para el proceso de selección se emplea un mecanismo de verificación de antecedentes ajustado a la ley, e informar la clasificación de información a la que tendría acceso el funcionario o contratista.
- Asegurar que para el proceso de selección y contratación se cuente con la autorización del tratamiento de datos personales por parte de los candidatos y funcionarios.
- Asegurar que todo funcionario y contratista acepte el acuerdo de confidencialidad y no divulgación y las políticas de la seguridad y privacidad de la información.
- Asegurar que todo funcionario y contratista conozca y acepte sus responsabilidades frente a la seguridad y privacidad de la información.
- Durante el proceso de inducción a nuevos funcionarios, incluir una charla de concientización con apoyo del grupo de gestión TI sobre los requisitos de seguridad y privacidad de la información, responsabilidades legales, uso correcto de los servicios de procesamiento de Información y procesos disciplinarios antes de que se les otorgue acceso a información o sistemas de información sensibles de la Secretaría de Educación y Cultura del Tolima.

Durante la ejecución del cargo

- Asegurar que todos los funcionarios y contratistas conozcan y acepten las políticas de seguridad y privacidad de la información, así como, entender y aceptar las consecuencias y medidas a tomar por el incumplimiento de estas.
- Generar campañas periódicas de capacitación y sensibilización en seguridad y privacidad de la información.
- Establecer un programa de toma de conciencia, educación y formación frente a las políticas, controles definidos y procedimientos de seguridad y privacidad de la información relacionados con los cargos desempeñados por funcionarios o contratistas.
- Monitorear el cumplimiento de las políticas y responsabilidades en materia de seguridad y privacidad de la información.
- Ofrecer la asesoría requerida por los funcionarios o contratistas en materia de seguridad y privacidad de la información.

- Realizar una revisión anual o cuando sea necesario del material de capacitación en seguridad y privacidad de la información, a fin de evaluar la actualización y vigencia de este.
- Definir un mecanismo anónimo de reporte frente al incumplimiento de políticas y procedimientos de seguridad y privacidad de la información.
- Garantizar que todos los perfiles de cargo incluyan las responsabilidades frente a la seguridad y privacidad de la información.
- Establecer un programa de toma de conciencia, educación y formación frente a las políticas, controles definidos y procedimientos de seguridad y privacidad de la información relacionados con los cargos desempeñados por funcionarios o contratistas.
- Establecer un proceso disciplinario formal, a través del cual se den a conocer y se apliquen las sanciones asociadas al incumplimiento o violación de las políticas y procedimientos de seguridad y privacidad de la información definidos por la organización.

Terminación y cambio de cargo

- Definir y comunicar un procedimiento a través del cual se informe de manera oportuna al Grupo de Gestión de TIC y Sistemas de Información y demás áreas interesadas el retiro de funcionarios y contratistas, para dar inicio al proceso de eliminación de usuarios y perfiles que les fueron asignados durante su permanencia en la Secretaría de Educación y Cultura y de los activos, incluyendo los activos de información bajo su cargo (datos, información impresa, aplicaciones / software, equipos informáticos / hardware, redes de comunicaciones, medios de almacenamiento, servicios, recurso humano, instalaciones, equipamiento auxiliar)

2.2. Política Uso Aceptable Activos Información

Objetivo:

El objetivo de estas políticas y responsabilidades es definir las reglas necesarias para realizar la identificación de los activos de información.

Políticas:

Un activo de información es un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como vital para la operación de la entidad; independiente del tipo de activo, se deben considerar las siguientes características:

- Los activos de información son reconocidos como valiosos por cada responsable del proceso.
- La Secretaria cuenta con herramientas que permite registrar y clasificar los activos de información de acuerdo con el marco normativo nacional.
- Asegurar la designación de los propietarios de los activos de información al momento de su creación o cuando son transferidos a la organización.
- Inventariar los activos de información (datos, información impresa, aplicaciones / software, equipos informáticos / hardware, redes de comunicaciones, medios de almacenamiento, servicios, recurso humano, instalaciones, equipamiento auxiliar) involucrados en el desarrollo de sus procesos y dentro del ciclo de vida de la información.
- Garantizar que los activos de información se encuentran clasificados de acuerdo con las pautas establecidas.
- Mantener un inventario de activos de información, de manera exacta y consistente. Este inventario debe ser actualizado al menos una vez por año.
- Establecer mecanismos de respaldo que garanticen la confidencialidad, integridad y disponibilidad de la información sensible alojada en los equipos de cómputo
- Adoptar los mecanismos de respaldo establecidos.

2.3. Política Clasificación y Manejo Información

Objetivo:

El objetivo de estas políticas y responsabilidades es establecer la normativa que le permitirá a los usuarios conocer qué medidas de protección mínimas aplicar para la clasificación y manejo de la información.

Políticas:

Un activo de información es un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como vital para la operación de la entidad; independiente del tipo de activo, se deben considerar las siguientes características:

- Definir el procedimiento para la asignación de activos de información a colaboradores y contratistas.
- Definir los mecanismos y procedimientos que garanticen el apropiado tratamiento de los activos de información al momento de su eliminación o destrucción (física y digital).
- Garantizar la asignación de los activos de información requeridos por colaboradores y contratistas para el desarrollo de sus funciones con base en el procedimiento definido.
- Garantizar que los propietarios de los activos de información sean colaboradores o procesos que tenga responsabilidad directa designada de la empresa sobre los mismos.
- Acoger los mecanismos y procedimientos definidos para la eliminación o destrucción de los activos de información.
- Validar de manera periódica las restricciones y clasificaciones de acceso a los activos importantes de acuerdo con las políticas de control de acceso aplicables.
- Garantizar la integridad, confidencialidad y disponibilidad de los activos.
- Garantizar el manejo apropiado del activo cuando es eliminado o destruido
- Definir las condiciones de uso y protección de los activos de información, tanto los tecnológicos como aquellos que no lo son para proteger su confidencialidad, integridad y disponibilidad.
- Cumplir y acoger con integridad las políticas de seguridad definidas por la organización para dar un uso racional y eficiente a los activos asignados que son propiedad de la Secretaría de Educación y Cultura del Tolima.

2.4. Política Control de Acceso

Objetivo:

El objetivo de estas políticas y responsabilidades es limitar el acceso a la información, de acuerdo a los roles de usuario específicos asignados a los funcionarios y contratistas con relación a los activos de información, estableciendo niveles de autorización y de acceso a los sistemas de información y en general a los activos de información.

Políticas:

- Garantizar el correcto uso de las cuentas y contraseñas de acceso a los sistemas ya que su uso es personal e intransferible.
- La creación de contraseñas seguras donde no se incluya información personal como nombres, fechas de nacimiento u otros de fácil conocimiento por terceros.
- Efectuar el cambio de sus contraseñas de acceso a los diferentes sistemas de manera periódica o cuando estos consideren que ha sido expuesta a terceros.
- Informar el retiro de los colaboradores y contratistas de la organización tan pronto esta se produzca para realizar la correspondiente eliminación de cuentas en los sistemas de información.
- Realizar una depuración periódica de las cuentas de acceso en cada uno de activos a los cuales aplique.
- Garantizar que los administradores de las soluciones de correo electrónico y herramientas colaborativas no visualicen las comunicaciones de los funcionarios y contratistas, a menos que exista una autorización judicial o de autoridad competente.
- Garantizar el control técnico de acceso a sitios que puedan afectar la productividad de la organización, la seguridad y privacidad de su información o su personal. Ningún colaborador, proveedor o contratista de la Secretaría de Educación y Cultura del Tolima está autorizado para realizar instalación de software en los dispositivos móviles o de escritorio de la organización. Toda solicitud al respecto debe ser escalada a través de requerimientos al grupo de gestión TI y ejecutada por personal de soporte técnico, previa autorización del personal del grupo TI.
- El Grupo de Gestión de TI y Sistemas de Información, es la única instancia encargada de autorizar el uso de herramientas tecnológicas para análisis de tráfico y hacking ético al interior de la Secretaría de Educación y Cultura del Tolima.

2.5. Política Seguridad física y del entorno

Objetivo:

Prevenir e impedir accesos no autorizados, daños, interrupciones e interferencias a las instalaciones, sedes e información de la Secretaría de Educación y Cultura del Tolima; controlar incendios, inundaciones, sobrecargas eléctricas, disturbios civiles y otras formas de desastres naturales o causadas por el hombre que podrían perjudicar el correcto funcionamiento de los recursos informáticos que albergan información.

Políticas:

- El área de Tecnología Informática y equipos informáticos de la Secretaría deben cumplir las políticas y procedimientos de seguridad física, con el fin de restringir el acceso a personal no autorizado y evitar daños e interferencias en la información y los recursos tecnológicos que la soportan.
- Documentar los procedimientos necesarios para garantizar la definición, instalación y monitoreo de perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información (Centro de Datos), de suministros de energía eléctrica (Planta Eléctrica), de aire acondicionado (Aire Central), cuartos técnicos y de cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.
- Definir y hacer cumplir las recomendaciones de seguridad para el ingreso a las instalaciones de procesamiento de información (Centro de Datos), de suministros de energía eléctrica (Planta Eléctrica), de aire acondicionado (Aire Central), cuartos técnicos y de cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.
- Garantizar la instalación y monitoreo de perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información (Centro de Datos), de suministros de energía eléctrica (Planta Eléctrica), de aire acondicionado (Aire Central), cuartos técnicos y de cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.
- Garantizar que las instalaciones de procesamiento de información tengan perímetros de seguridad construidos con base en las buenas prácticas nacionales e internacionales (techos, paredes, pisos, puertas de acceso, ventanas.
- Supervisar o inspeccionar a los visitantes de áreas protegidas, validar su identidad y registrar la fecha y hora de ingreso y salida del lugar. Sólo se permitirá el acceso para

propósitos específicos y autorizados, notificando al visitante al momento del ingreso sobre los requisitos de seguridad del área y los procedimientos de emergencia.

- Limitar y controlar el acceso a la información y a las instalaciones de procesamiento de información sólo para personal autorizado a través de controles electrónicos, biométricos o físicos. Los controles generarán un registro protegido para permitir auditar todos los accesos.
- Garantizar que los funcionarios, proveedores, contratistas y visitantes de la Secretaría de Educación y Cultura del Tolima porten de manera visible el carné de la Institución.

2.6. Política Seguridad de las operaciones de gestión tecnológica

Objetivo:

Definir las reglas y requerimientos que deben cumplir los funcionarios, proveedores y contratistas de la Secretaría de Educación y Cultura del Tolima para poder garantizar el funcionamiento adecuado, correcto y seguro de las instalaciones de procesamiento de la información y las comunicaciones de la Secretaría de Educación y Cultura del Tolima. Estas reglas y requerimientos están definidos con el fin de proteger la confidencialidad, integridad y disponibilidad de la información que se maneja en las instalaciones de procesamiento y también poder asegurar que los cambios que se efectúen sobre los recursos tecnológicos sean controlados de forma adecuada y debidamente autorizados.

Políticas:

- Garantizar que se definan, comuniquen y mantengan actualizados los procedimientos operativos asociados con las instalaciones de procesamiento y comunicación de la Secretaría de Educación y Cultura del Tolima, los cambios de estos procedimientos solo serán autorizados por esta dirección.
- Garantizar que se definan, comuniquen y mantengan actualizados los procedimientos para el control de los cambios en el ambiente productivo y de comunicaciones de la Secretaría de Educación y Cultura del Tolima. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad por parte del Comité de Control de Cambios definido al interior, a menos que se considere un cambio estándar.
- Asegurar que se conserve un registro de auditoría que contenga toda la información relevante de cada cambio implementado (Herramienta de Control de Cambios definida por la Organización).
- Asegurar que los cambios que se lleven a cabo sean evaluados y probados de forma integral y que se cuente con la participación de los líderes de los procesos usuarios, a fin de revisar y garantizar la funcionalidad de los cambios realizados en los diferentes componentes de la solución.
- Garantizar que se definan, comuniquen y mantengan actualizados los procedimientos asociados con la gestión de la capacidad de la demanda de los sistemas en operación, de los recursos humanos, oficinas e instalaciones y la proyección de futuras demandas, con el fin de garantizar un procesamiento y almacenamiento adecuado e ininterrumpido.
- Generar ajustes, mejoras, mantenimientos y/o planes de acción, resultado del monitoreo y gestión de la capacidad, que permitan garantizar la continuidad en la prestación del servicio de la organización y minimizar la posibilidad de ocurrencia de eventos de no disponibilidad.

Separación de los ambientes de desarrollo, pruebas y producción

- Garantizar que exista una separación física y lógica de los ambientes de desarrollo, pruebas y producción; con el fin de reducir los riesgos de cambio accidental o acceso no autorizado al software operacional y a la información clasificada como confidencial o de uso interno.
- Garantizar que se definan, comuniquen y mantengan actualizados los procedimientos asociados con la transferencia de software del estatus de desarrollo al de producción.
- Garantizar que se definan, comuniquen y mantengan actualizados los procedimientos que aseguren que los cambios en los sistemas de producción y aplicaciones se han puesto en prueba, en un ambiente de pruebas antes de aplicarlos en el ambiente de producción.
- Garantizar que se impida el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente de producción, cuando no sean indispensables para su funcionamiento.
- Garantizar que los usuarios usen diferentes perfiles en los sistemas de producción y de pruebas, y los menús deberían mostrar mensajes de identificación apropiado con el fin reducir el riesgo de error.
- Garantizar que los datos clasificados como confidenciales no sean copiados en el ambiente de pruebas o desarrollo sin el proceso de transformación o enmascaramiento correspondiente con el fin de reducir el acceso no autorizado o robo de esta información.

Protección contra códigos maliciosos

- Garantizar que todos los dispositivos móviles y de escritorio sólo cuenten con software autorizado por la organización.
- Garantizar la prohibición y detección del uso de sitios web maliciosos o que se sospecha.
- Evitar la descarga de archivos y software desde o a través de redes externas, o por cualquier otro medio.
- Garantizar que se definan, comuniquen y mantengan actualizados los procedimientos que ayuden a reducir las vulnerabilidades de las cuales pueda aprovecharse el software malicioso.
- Garantizar que se realiza una revisión periódica del contenido de software y datos de los equipos que apoyan los procesos críticos de la Secretaría de Educación y Cultura del Tolima, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
- Garantizar que se realice de forma continua un análisis de los computadores y medios de la Secretaría de Educación y Cultura del Tolima, con el fin de protegerlos contra código malicioso. El análisis debe incluir cualquier archivo recibido por la red o cualquier

medio de almacenamiento antes de su uso, el análisis de los adjuntos y descargas de los correos electrónicos antes de su uso y el análisis de páginas web.
- Garantizar la instalación y actualización regular del software de detección y reparación del software malicioso en los equipos portátiles, de escritorio y de procesamiento.
- Generar campañas periódicas de capacitación y sensibilización en seguridad y privacidad de la información, con el fin de dar a conocer las precauciones apropiadas acerca de los peligros y amenazas de los códigos maliciosos y de los controles con los que cuenta la organización para mitigar los riesgos de estos.

Respaldo de la información

Determinar los requisitos para copias de respaldo de la información y los sistemas en función de su criticidad y clasificación. Con base a ello, se definirá y documentará un esquema de retención y protección.

Registro de eventos

- Determinar los eventos que generarán un registro de auditoria de los sistemas y equipos de la Secretaría de Educación y Cultura del Tolima.
- Asegurar la integridad, confidencialidad y disponibilidad de los registros de auditoria de los sistemas y equipos de la Secretaría de Educación y Cultura del Tolima.
- Conservar y revisar regularmente los registros (Logs) acerca de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Protección de la información de registro

- Asegurar que en donde sea posible, los administradores de sistemas no tengan permiso para borrar o desactivar registros de auditoria de sus propias actividades.
- Asegurar que los registros de auditoria serán archivados preferentemente en un equipo diferente al que los genere y conforme los requerimientos de retención de registros.

Registros del administrador y del operador

- Asegurar el registro de las actividades realizadas por los operadores y administradores de los sistemas de la Secretaría de Educación y Cultura del Tolima.
- Contrastar los rastros de las actividades realizadas por los operadores y administradores en
- relación con los procedimientos descriptivos de sus labores.

Sincronización de relojes

- Garantizar que se defina, comunique y mantenga actualizado el procedimiento que asegure el ajuste de relojes de los equipos, el cual contemplará la verificación de estos contra el Instituto Nacional de Metrología; estableciendo los correctivos ante cualquier variación significativa, con el fin de evitar que los registros de auditoria que puedan ser necesarios para investigaciones sean inexactos y puedan dificultar estas investigaciones y afectar la credibilidad de la evidencia.

Control de software operacional

- Que se defina, comunique y mantenga actualizado el procedimiento que asegure el control sobre la instalación de actualizaciones en sistemas operativos.
- Que los sistemas operativos sólo contengan códigos ejecutables aprobados y no el código de desarrollo o compiladores.
- Antes que cualquier sistema operativo sea puesto en operación en la organización, se debe aplicar las líneas base de seguridad.
- Que se defina, comunique y mantenga actualizado el procedimiento con el cual se lleve un control de la configuración, con el fin de mantener un control de todo el software implementado, al igual que la del sistema operativo.

Gestión de la vulnerabilidad técnica

- Mantener un inventario actualizado y completo de los activos de información.
- Garantizar que se defina, comunique y mantenga actualizado el procedimiento que asegure una gestión eficaz para las vulnerabilidades técnicas que sean identificadas.
- Garantizar que se realice un escaneo semanal a todos los activos definidos como críticos haciendo uso del hardware de propósito específico definido por la Secretaría de Educación y Cultura del Tolima para este propósito.
- Presentar un informe periódico sobre el estado de las vulnerabilidades para los activos críticos definidos por las empresas de la Secretaría de Educación y Cultura del Tolima.
- Garantizar que los indicadores de riesgo de los activos críticos se mantengan en el nivel definido por el Comité directivo ampliado.
- Gestionar que el cierre o mitigación de las vulnerabilidades se realice en los tiempos definidos por el Comité directivo ampliado.
- Garantizar que las labores de tratamiento de las vulnerabilidades deben gestarse en coherencia con los procedimientos definidos para el control de los cambios.
- Realizar una revisión periódica (mensual) sobre la gestión de vulnerabilidades.

2.7. Política Seguridad de las comunicaciones

Objetivo:

Definir los responsables de desarrollar los procedimientos e implementar los controles que eviten los daños e interferencias a la información de la Secretaría de Educación y Cultura del Tolima, las instalaciones de procesamiento de la información y ayuden a mantener la seguridad de la información que transfiere la Secretaría de Educación y Cultura del Tolima internamente o con entidades externas.

Políticas:

- Garantizar que la responsabilidad operacional de las redes esté separada de las operaciones de cómputo.
- Garantizar la implementación de controles para asegurar la confidencialidad e integridad de la información que viaja sobre redes públicas o inalámbricas, para proteger los sistemas y aplicaciones conectados.
- Garantizar que los mecanismos de autenticación adecuados se aplican a los usuarios y equipos.
- Garantizar el cumplimiento del control de los accesos de los usuarios a los servicios de información.

Políticas y procedimientos de transferencia de información

- Garantizar que se defina, comunique y mantenga actualizado los procedimientos para proteger la información transferida contra interceptación, copiado, modificación, enrutado y destrucción.
- Garantizar que se defina, comunique y mantenga actualizado los controles para la detección de software malicioso y protección contra éste, que pueda ser transmitido mediante el uso de comunicaciones electrónicas.
- Hacer gestión para que se utilicen las técnicas de cifrado adecuadas para proteger la confidencialidad, integridad y autenticidad de la información.
- Garantizar que se definan, comuniquen y mantengan actualizados los procedimientos para evitar que se tenga acceso no autorizado a los mensajes almacenados en equipos multifuncionales y teléfonos IP que estén bajo su gestión.
- Garantizar que se definan, comuniquen y mantengan actualizados los procedimientos para evitar que se logren programar las máquinas o servicios de fax de forma deliberada o accidental para enviar mensajes a números específicos.
- Generar campañas periódicas de capacitación y sensibilización en seguridad y privacidad de la información, con el fin de dar a conocer las precauciones apropiadas

acerca de no revelar información confidencial o de uso interno por cualquier medio de comunicación.

- Generar campañas periódicas de capacitación y sensibilización en seguridad de la información, con el fin de dar a conocer las precauciones apropiadas acerca de no tener conversaciones confidenciales en lugares públicos, o mediante canales de comunicación no seguros, oficinas abiertas y lugares de reunión.
- Generar campañas periódicas de capacitación y sensibilización en seguridad y privacidad de la información, con el fin de dar a conocer las precauciones apropiadas acerca de no dejar información expuesta en dispositivos de impresión, reproducción, copiado, escaneo, duplicado, facsímil, contestadores telefónicos automáticos u otros.
- Asegurar que no se deja ningún tipo de mensaje que contenga información confidencial o de uso interno, en las máquinas contestadoras, debido a que estos mensajes pueden ser escuchados por personas no autorizadas.

Acuerdos sobre transferencia de información

- Definir cómo se debe realizar el intercambio de información con terceros, según los acuerdos de intercambio y cumplir con la legislación correspondiente, con el fin de proteger la integridad y confidencialidad de la información.
- Definir, revisar y firmar los acuerdos de confidencialidad e intercambio de información que se puedan dar entre la Secretaría de Educación y Cultura del Tolima y terceros.
- Realizar la autorización para el establecimiento de un vínculo de transmisión de información con terceros.

Mensajería electrónica

- Garantizar que se definan, comuniquen y mantengan actualizados los procedimientos que garanticen la protección adecuada de la información incluida en la mensajería electrónica (correo electrónico, intercambio electrónico de datos y redes sociales).

2.8. Política Adquisición, Desarrollo y Mantenimiento De Sistemas

Objetivo:

- Asegurar que durante todo el ciclo de vida de desarrollo de los sistemas de información se incluyan los requerimientos de seguridad y privacidad de la información con el fin de lograr sistemas de información más seguros y capaces de resistir ataques.

Políticas:

- Garantizar que los desarrollos y mejoras sobre los sistemas de información apliquen metodologías de desarrollo seguro durante todo el ciclo de vida (Análisis, Diseño, Codificación, Pruebas, Implementación y Mantenimiento), que permitan garantizar aplicaciones de calidad desde el propio inicio del proyecto, contemplando los criterios de confidencialidad, integridad, disponibilidad y privacidad.
- Asegurar que se realicen las actividades de identificación de requerimientos de seguridad y privacidad de la información, teniendo en cuenta las políticas de seguridad y privacidad de la información, estándares, regulaciones y aspectos legales.
- Asegurar que durante la fase de diseño se tengan presentes los requerimientos de seguridad y privacidad de la información para la construcción de los controles de seguridad, tales como: controles de acceso, opciones de cifrado, aspectos de continuidad de negocio, registros de auditoría, etc.
- Asegurar que las aplicaciones desarrolladas cuenten con una matriz de roles al momento de su entrega, con el objetivo de facilitar el levantamiento de la matriz de perfiles por cargo.
- Disponer las herramientas tecnológicas que permitan detectar fallas de seguridad en el código fuente de las aplicaciones desarrolladas al interior o por parte de terceros.
- Garantizar que, durante la fase de pruebas de los nuevos sistemas de información o mejoras realizadas sobre estos, sean expuestos a procesos de análisis de penetración o escaneo de vulnerabilidades antes de salir a producción.
- Considerar antes de la adquisición de cualquier sistema de información, el riesgo introducido y los controles asociados a los sistemas que no cumplan con los requisitos de seguridad y privacidad de la información.

Seguridad de servicios de las aplicaciones en redes públicas

- Garantizar que la información involucrada en los servicios de aplicaciones que viaja a través de redes públicas se debe proteger de actividades fraudulentas.

Protección de transacciones de los servicios de las aplicaciones

- Hacer gestión para proteger la información involucrada en las transacciones de los servicios de las aplicaciones para evitar alteraciones en la información o divulgación no autorizada.

Seguridad en los procesos de desarrollo y de soporte

- Adoptar procedimientos de desarrollo seguro de software o de sistemas, para el software que se construya al interior de la organización.

Procedimientos de control de cambios en sistemas

- Garantizar que se definan, comuniquen, apliquen y mantengan actualizados los procedimientos para el control de los cambios durante el ciclo de vida de desarrollo de software o de sistemas.

Revisión técnica de las aplicaciones después de cambios en la plataforma de operación

- Garantizar que cada vez que se realice un cambio en la plataforma de operación (sistema operativo, bases de datos o software de capa media) se revisen los sistemas de la Secretaría de Educación y Cultura del Tolima para evitar que se produzca un impacto en su funcionamiento y en la seguridad.
- Garantizar que durante la revisión técnica de las aplicaciones se tenga presente las siguientes consideraciones:

    - Revisar los procedimientos de integridad y control de aplicativos para garantizar que no hayan sido comprometidos por el cambio.
    - Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación
    - Asegurar la actualización del plan de continuidad de las actividades de la Secretaría de Educación y Cultura del Tolima.

Restricciones en los cambios a los paquetes de software

- Asegurar que cualquier modificación de paquetes de software suministrados por proveedores a la Secretaría de Educación y Cultura del Tolima considere los siguientes lineamientos:
- Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
- Determinar la conveniencia de que la modificación sea efectuada internamente, por el proveedor o por un tercero calificado.
- Evaluar el impacto que se produce si la organización se hace cargo del mantenimiento de la aplicación por los cambios efectuados.

- Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

Principios de construcción de sistemas seguros

- Ejecutar procesos de análisis de riesgos durante la fase de construcción.
- Incluir la seguridad en el diseño de todas las capas de arquitectura (negocio, datos, aplicaciones y tecnología), con el fin de equilibrar la necesidad de seguridad de la información con la necesidad de accesibilidad.
- Realizar una revisión del diseño de la aplicación y problemas relacionados a la arquitectura, para detectar problemas de manera temprana en el proceso de desarrollo de la aplicación, antes de que sea liberada.
- Garantizar la revisión o verificación del código fuente de la aplicación para detectar huecos de seguridad.
- Aplicar metodologías para el desarrollo de aplicaciones seguras y capaces de resistir ataques.

Ambiente de desarrollo seguro

- Establecer ambientes de desarrollo seguros para las labores de desarrollo de sistemas específicos, considerando:

    - Los controles de seguridad ya implementados por la organización, que brindan soporte al desarrollo del sistema.
    - La sensibilidad de los datos a procesar, almacenar y trasmitir.
    - El control de acceso al ambiente de desarrollo.
    - El control sobre el movimiento de datos desde y hacia el ambiente de desarrollo.

- Una vez se determine el nivel de protección para un ambiente de desarrollo, debe documentar los procesos correspondientes en procedimientos de desarrollo seguro y suministrarlos a todos los individuos que los necesiten.

Desarrollo contratado externamente

- Supervisar y realizar seguimiento a la actividad de desarrollo de los sistemas de información contratados externamente.
- Considerar los requisitos contractuales para prácticas seguras de diseño, codificación y pruebas.

- Garantizar que las fábricas de software cumplan con los principios de construcción de sistemas seguros, al igual que los definidos por la organización.
- Velar por el cumplimiento de las leyes que apliquen a las diferentes soluciones de sistemas de información en la organización aun cuando sean desarrollados por entes externos.
- Definir acuerdos sobre licencias, propiedad de los códigos y derechos de propiedad intelectual.
- Incluir contractualmente las pólizas de cumplimiento y calidad del trabajo realizado.
- Incluir derechos contractuales para auditar la calidad y exactitud del trabajo realizado.
- Definir requisitos contractuales sobre la calidad, seguridad y funcionalidad del código.
- Incluir dentro de los contratos con terceros que estos deben cumplir con las políticas de seguridad y privacidad de la información.
- Siempre que se contrate un externo para el desarrollo de software se debe exigir lo siguiente:
- Firmas de acuerdos de confidencialidad. Con esto se previene al tercero divulgar información crítica de la Empresa.
- Certificación de seguridad en el proceso de desarrollo. El tercero debe garantizar que su proceso de desarrollo recoge las mejores prácticas para el desarrollo seguro de aplicaciones.
- Contratos de entrega de producto. En estos contratos se garantiza la aceptabilidad del producto final. Se debe incluir que los criterios de aceptación incluyen las pruebas funcionales, las pruebas de seguridad (casos de abuso y test de intrusión). Dichas pruebas deben ser exitosas y se deben hacer las correcciones pertinentes respecto a cualquier hallazgo encontrado.
- Inclusión de los requerimientos de seguridad y privacidad. Los terceros deben entregar un producto que cumpla con el numeral de “Requisitos de seguridad y privacidad de los sistemas de información” del presente documento.
- Certificación libre de malware. El proveedor debe certificar que el producto entregado se encuentra libre de malware, troyanos o puertas traseras que pueden poner en peligro la seguridad del sistema de información.
- Auditorias. El proveedor debe permitir procesos de auditorías por la organización. Este tipo de auditoría debe estar orientada a la verificación del proceso de desarrollo del proveedor y que cumpla la definición de requerimientos de seguridad de la aplicación y que se ejecute las pruebas de seguridad.

Pruebas De Seguridad De Sistemas

- Desarrollar un programa de pruebas de seguridad efectivo que cuente con componentes que comprueben: las personas (para asegurarse de que se tiene la educación y concientización adecuadas), los procesos (para asegurarse que existen las

políticas y estándares adecuados, y que las personas saben cómo seguir dichas políticas), la tecnología (para asegurarse de que el proceso ha sido efectivo en su implementación) y de esta manera poder prever incidentes o problemas que más tarde se pueden manifestar en forma de defectos en la tecnología; y así erradicar bugs de forma temprana e identificar las causas de los defectos.

- Realizar pruebas de seguridad sobre las aplicaciones nuevas en las fases de Análisis, Diseño, Codificación, Pruebas, Implementación y Mantenimiento para descubrir vulnerabilidades y establecer un estándar mínimo para la liberación de la aplicación.
- Realizar pruebas de vulnerabilidad a las aplicaciones críticas de la organización cada mes con el fin de poder generar planes de acción para mitigar las vulnerabilidades detectadas. Cuando se realicen cambios en los sistemas, deberá realizarse una prueba adicional.
- Producir un registro formal de que comprobaciones se han realizado, y los detalles de los hallazgos. El reporte debe ser claro para los líderes de proceso o propietarios de la información, desarrolladores y personal de seguridad de la información.

Prueba de aceptación de sistemas

- Definir los criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva. Estas pruebas deben incluir las pruebas de requisitos de seguridad de la información y la adherencia a prácticas de desarrollo seguro.
- Asegurar que se cuente con ambientes de pruebas iguales a los ambientes de producción para evitar que se introduzcan vulnerabilidades al ambiente de producción.
- Los líderes de proceso, funcionarios deben participar y mantener la seguridad de la información en las pruebas y usuarios de pruebas para nuevos sistemas de información, actualizaciones y nuevas versiones, antes de su aprobación definitiva.

Datos de prueba

- Llevar un registro de autorización formal otorgada por el propietario de la información para realizar copias de la información operativa a los ambientes de prueba.
- Alterar (enmascaramiento) de los datos productivos cuando sea necesario utilizarlos en procesos de pruebas, de tal forma que no se pueda realizar una asociación entre la información de pruebas y producción.
- Hacer gestión para evitar el uso de datos operacionales que contengan información de datos personales o confidenciales para efectos de pruebas.
- Eliminar a la mayor brevedad y una vez completadas las pruebas, la información operativa utilizada.

2.9. Política Relaciones con los proveedores

Objetivo:

Definir lineamientos que garanticen la protección de los activos de información a los cuales tienen acceso proveedores y contratistas de la Secretaría de Educación y Cultura del Tolima y asegurar el cumplimiento de los acuerdos de seguridad de la información establecidos con los proveedores de la Secretaría de Educación y Cultura del Tolima.

Políticas:

- Asegurar que todos los proveedores con los cuales se establecerá relación conozcan y acepten las políticas, normas y procedimientos de seguridad y privacidad de la información establecidos por la Secretaría de Educación y Cultura del Tolima.
- Mantener una base de datos actualizada de los proveedores que tienen relación con la Secretaría de Educación y Cultura del Tolima y los tipos de productos y servicios ofrecidos.
- Definir un proceso y ciclo de vida para la gestión de las relaciones con los proveedores.
- Incluir dentro de todos los términos de referencia que se publiquen para adquisición de bienes y servicios de tecnología de la información y de comunicaciones, los requisitos de seguridad y privacidad de la información.
- Obtener de los proveedores la autorización del tratamiento de datos personales.
- Definir las finalidades para las cuales permitirá el acceso de información de la Secretaría de Educación y Cultura del Tolima al proveedor y responsabilidades para su tratamiento y uso.
- Garantizar que los proveedores extranjeros proporcionen los niveles adecuados de protección de datos personales.
- Firmar acuerdos de confidencialidad con los proveedores que permita tener el soporte del conocimiento y aceptación de las políticas, normas y procedimientos de seguridad y privacidad de la información establecidos por la Secretaría de Educación y Cultura del Tolima.

2.10. Política Gestión de Incidentes de seguridad y privacidad de la información

Objetivo:

Definir los lineamientos para la gestión eficaz de los eventos e incidentes de seguridad y privacidad de la información al interior de la Secretaría de Educación y Cultura del Tolima.

Políticas:

- Definir y comunicar los procedimientos que garanticen el reporte, detección, análisis, evaluación, respuesta y seguimiento de eventos e incidentes de seguridad y privacidad de la información reportados por los funcionarios, proveedores y contratistas y unidades de la Secretaría de Educación y Cultura del Tolima.
- Analizar, revisar y dar respuesta a los eventos e incidentes de seguridad y privacidad de la información reportados por los funcionarios, contratistas y proveedores de la Secretaría de Educación y Cultura del Tolima; de manera rápida, eficaz y ordenada.
- Definir y comunicar los procedimientos que garanticen el manejo de evidencia forense relacionada con los incidentes de seguridad y privacidad de la información.
- Revisar y documentar las lecciones aprendidas de la gestión de incidentes de seguridad y privacidad de la información con el fin de reducir la probabilidad de incidentes futuros que tengan una causa u origen similar.
- Documentar las pruebas que se programen sobre el esquema de gestión de incidentes de seguridad y privacidad de la información definido por la Secretaría de Educación y Cultura del Tolima.
- Presentar ante el Comité Directivo ampliado los incidentes de seguridad y privacidad de la información, con el fin de conocer las tendencias, categorías y tratamiento de estos, sin perjuicio de las líneas de reporte que formalmente se establezcan al interior.
- Definir una lista de posibles proveedores de servicios especializados de consultoría y análisis forense digital.
- Informar a los titulares de la información sobre la situación presentada y sus consecuencias cuando estén relacionadas con sus datos personales a través de los canales definidos por la organización.
- Proveer a todos los funcionarios, proveedores y contratistas de una sensibilización que incluya la identificación y reporte de los eventos que afectan la seguridad y privacidad de la información.

Evaluación de eventos de seguridad y privacidad de la información

- Revisar y analizar los eventos reportados, con el fin de iniciar la gestión y categorización sobre aquellos que realmente puedan considerarse como un incidente de seguridad y privacidad de la información.

- Analizar los eventos reportados por los usuarios internos y externos de la Secretaría de Educación y Cultura del Tolima, y definir si estos efectivamente representan un incidente de seguridad y privacidad de la información para el trámite correspondiente de los mismos.
- Documentar en forma detallada el incidente, con el fin dar respuesta al mismo.
- Categorizar el incidente documentado para el manejo estadístico correspondiente.

Recolección de evidencia

- Coordinar la contratación y realización de una Investigación Forense que permita identificar a detalle el origen, responsable y comportamiento del incidente (cuando sea requerido). De igual forma, garantizar la cadena de custodia correspondiente en caso de que el incidente tenga un tratamiento judicial.

Respuesta a incidentes de seguridad y privacidad de la información

- Dar respuesta a los incidentes de seguridad y privacidad de la información dentro de los tiempos acordados según su criticidad e impacto.
- Garantizar la recuperación del negocio ante el incidente presentado.
- Reportar de forma inmediata a los titulares de la información (clientes, funcionarios, contratistas y proveedores) los incidentes presentados sobre sus datos personales, las consecuencias asociadas a los mismos y los mecanismos que podría adoptar para disminuir el daño potencial.
- Reportar de forma oportuna a la Superintendencia de Industria y Comercio (SIC) los incidentes presentados sobre los datos personales de los titulares de la información; los cuales deberán contener como mínimo la siguiente información: tipo de incidente, fecha y hora de ocurrencia, fecha y hora de descubrimiento, causa, tipo de datos personales comprometidos y cantidad de datos personales de los titulares afectados.
- Recolectar información del incidente para soportar el reporte correspondiente ante la SIC.

Aprendizaje obtenido de los incidentes de seguridad y privacidad de la información

- Documentar las lecciones aprendidas resultantes del proceso de gestión de incidentes, con el objetivo de garantizar la base de conocimiento.
- Realizar como mínimo una (1) vez al año la revisión y mejora de los procesos de gestión de riesgos y gestión de incidentes de seguridad y privacidad de la información apoyados en las lecciones aprendidas que han sido documentadas.

2.11. Políticas para Usuarios Finales

Objetivo:

Dar a conocer las políticas que deben adoptar todos los funcionarios, proveedores y contratistas que permita controlar y proteger la información de la Secretaria.

Políticas:

- Garantizar el correcto uso de las cuentas y contraseñas de acceso a los sistemas ya que su uso es personal e intransferible.
- La creación de contraseñas seguras donde no se incluya información personal como nombres, fechas de nacimiento u otros de fácil conocimiento por terceros.
- Efectuar el cambio de sus contraseñas de acceso a los diferentes sistemas de manera periódica o cuando estos consideren que ha sido expuesta a terceros.
- Abstenerse de utilizar la cuenta de correo corporativo para la recepción o envío de mensajes de tipo personal.
- Asegurar que todas las comunicaciones laborales que se realicen a través de correo electrónico, tanto internas como externas, se efectúen solamente a través de la cuenta de correo electrónico corporativa.
- Respetar la privacidad de las cuentas de correo y evitar el envío de mensajes desde cuentas de otros usuarios.
- Garantizar que toda la información confidencial o de uso interno que deba ser transmitida a través de correo electrónico, emplee mecanismos de cifrado fuerte / certificados digitales y a través de las redes de datos y sistemas internos únicamente.
- Abstenerse de utilizar el servicio de correo corporativo para la transmisión de cualquier correo masivo no solicitado, ya que el área autorizada para realizar este tipo de difusiones es el responsable de las comunicaciones.
- Abstenerse de enviar mensajes a través de correo electrónico o mensajería instantánea, que ofendan la dignidad, intimidad y buen nombre de las personas, de las instituciones, o para realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil; de igual forma se prohíbe difundir ideas políticas, religiosas, propagandas entre otros.
- Aplicar los lineamientos para el etiquetado de la información de la Secretaría de Educación y Cultura del Tolima soportada en formatos físicos o electrónicos.

- Utilizar el servicio de internet con propósitos lícitos y en cumplimiento de las funciones específicas de su cargo; toda actividad de navegación es registrada, quien podrá revelar cualquier acceso cuando una autoridad judicial así lo requiera.
- Evitar el acceso y abandonar sitios de internet catalogados como de baja reputación.
- Evitar la descarga de software de Internet de sitios desconocidos.
- Abstenerse de descargar y usar software malicioso o documentos que brinden información sobre cómo atentar contra la seguridad y privacidad de la información de la organización.
- Abstenerse de alojar cualquier tipo de información sensible en sitios de Internet que ofrezcan servicios para almacenar y/o compartir información, si no se encuentra cifrada la información mediante los mecanismos definidos.
- Evitar la descarga y/o emplear archivos de imagen, sonido o similares que puedan estar protegidos por derechos de autor sin la previa autorización.
- Garantizar la devolución de los activos de información asignados a colaboradores y contratistas para el desarrollo de sus funciones al terminar su relación laboral, este debe contemplar la entrega de elementos físicos, elementos electrónicos e información.
- No prestar el carné de acceso ya que es de uso personal e intransferible, siendo considerados como una contraseña de acceso físico.
- Garantizar la revisión periódica de las áreas seguras, al igual que cerrarlas con llave cuando estas se encuentren vacías.
- Garantizar que no se haga uso de equipo fotográfico, de video, audio u otro equipo de grabación (cámaras en dispositivos móviles) dentro de las áreas seguras a menos que se cuente con la autorización respectiva.
- Garantizar el cierre de las sesiones de aplicación y servicios de red cuando ya no sean requeridos.
- Garantizar el bloqueo de los equipos que se encuentren conectados a la red corporativa cuando deje desatendido el equipo.
- Escritorios Limpios: Garantizar que no se publique o se deje a la vista información sensible de acceso a los diferentes sistemas, como por ejemplo contraseñas, contratos, números de cuenta, plantas, historias laborales, datos de funcionarios y todo aquello que no se desea publicar.
- Garantizar que la información confidencial o de uso interno (papeles, medios de almacenamiento electrónico, etc.) permanezca guardada cuando no se requiera (caja fuerte o gabinete con llave); y especialmente cuando la oficina se encuentre desocupada.
- Garantizar que la información confidencial o de uso interno se retire de manera inmediata de los equipos multifuncionales.

- Cada vez que se requiera utilizar USB en los equipos de la secretaria, esta debe ser escaneada.
- No instalar software en los equipos de la secretaria.
- Para salvaguardar la información el medio es el ONEDRIVE de la herramienta OFFICE 365, la cual es la plataforma oficial de la Secretaría de Educación y Cultura del Tolima.
- Se debe incorporar el análisis de riesgos y las definiciones de los controles de seguridad de la información en todos los proyectos que inicien en la Secretaria de Educación y Cultura del Tolima.

Reporte de eventos y debilidades de seguridad y privacidad de la información

- Todos los funcionarios deben reportar al correo seguridaddigital@sedtolima.gov.co los eventos e incidentes de seguridad y privacidad de la información que son ocasionados por accidentes, errores o actos maliciosos intencionados, robo, apropiación indebida, extorsión, fraude, espionaje o eventos ambientales;
- Todos los funcionarios deben preservar la confidencialidad de la información relacionada con el manejo, investigación y seguimiento de los incidentes de seguridad y privacidad de la información.

2.12. Política Gestión de Continuidad del Negocio.

Objetivo:

Preservar los requisitos de seguridad y privacidad de la información en los procesos de continuidad de negocio y recuperación de desastres durante todas las fases de planeación, respuesta y recuperación.

Políticas:

- Determinar los requisitos de seguridad y privacidad de la información durante el desarrollo de los planes de continuidad de negocio y planes de recuperación de desastres.
- Establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad y privacidad de la información durante una situación adversa.
- Establecer, implementar y mantener controles de seguridad y privacidad de la información alternos cuando los controles definidos en situación normal no garanticen la seguridad y privacidad de la información en situaciones adversas.
- Desarrollar y aprobar los planes de respuesta y recuperación donde se detalle como la organización gestionará un evento perturbador y mantendrá la seguridad y privacidad de la información en un nivel aceptable con base en los objetivos definidos en la fase de planificación.
- Revisar los controles de continuidad de la seguridad y privacidad de la información definidos e implementados, con el objetivo de corroborar que son válidos y eficaces durante situaciones adversas, se recomienda realizar estas pruebas junto con las pruebas de continuidad de negocio y recuperación de desastres.
- Revisar los controles de continuidad de la seguridad y privacidad de la información definidos e implementados, con el objetivo de corroborar que son válidos y eficaces durante situaciones adversas a través de planes de pruebas de continuidad y recuperación ante desastres.

Redundancias

- Deben contemplar soluciones de redundancia para los sistemas de apoyo a los procesos críticos con el fin de garantizar los requisitos de disponibilidad.

- Deben realizar pruebas periódicas de los sistemas de información que cuenten con redundancia para asegurar que después de una falla, el paso de operación de un componente a otro funcione de manera correcta.

2.13. Política Cumplimiento, Requisitos Legales Contractuales

Objetivo:

Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con la seguridad y privacidad de la información y de cualquier requisito de seguridad.

Políticas:

- Identificar los requisitos legales, estatutarios, reglamentarios y contractuales aplicables de la Secretaría de Educación y Cultura del Tolima en materia de seguridad y privacidad de la información con el fin de garantizar el cumplimiento de estos.
- Definir y comunicar los procedimientos que garanticen la privacidad de la información de los funcionarios, proveedores, contratistas y clientes de la Secretaría de Educación y Cultura del Tolima por parte de los responsables y encargados del tratamiento de datos personales de la organización.
- Definir e implementar una política de protección de datos personales corporativa que cumpla los requisitos legales.
- Definir e implementar un aviso de privacidad que comunique a los Titulares de los datos personales, las finalidades del tratamiento de acuerdo con los requisitos legales.
- Establecer las finalidades del tratamiento de los datos personales de los grupos de interés de la Secretaría de Educación y Cultura del Tolima.
- Establecer y habilitar los medios para el ejercicio de los derechos de los Titulares de datos personales.
- Determinar los procedimientos necesarios para el tratamiento de los datos personales de categoría especial (datos sensibles y de menores de edad) que permitan garantizar su seguridad.
- Definir y comunicar los procedimientos que garanticen el cumplimiento de los derechos de propiedad intelectual y el uso de software legal por parte de los funcionarios, proveedores y contratistas de la Secretaría de Educación y Cultura del Tolima.
- Garantizar la adquisición de software a través de proveedores autorizados para asegurar el respeto a los derechos de autor.
- Definir, comunicar y aplicar sanciones frente al incumplimiento de derechos de propiedad intelectual y uso de software legal por parte de los funcionarios y contratistas y unidades de la Secretaría de Educación y Cultura del Tolima.

- Definir, comunicar y aplicar sanciones a los funcionarios y contratistas frente al incumplimiento de los procedimientos que garantizan la protección de datos personales al interior de la organización.
- Definir los procedimientos necesarios que garanticen la adecuada administración de los activos de software y unidades de la Secretaría de Educación y Cultura del Tolima, al igual que emisión de reportes periódicos (mensuales) sobre el estado de legalidad de software. Garantizar el uso de controles criptográficos dentro de los procesos transporte, procesamiento y almacenamiento de información sensible dentro de la red corporativa; al igual que en los procesos de intercambios de información con terceros.
- Velar por que, en el uso, captura, recolección y tratamiento de datos personales, se garantice la calidad y veracidad de la información.
- Verificar que se adopten las medidas tecnológicas y administrativas necesarias para evitar la adulteración, modificación, pérdida, consulta, uso o acceso no autorizado a los registros y repositorios de la Secretaría de Educación y Cultura del Tolima.
- Identificar los requisitos legales, estatutarios, reglamentarios y contractuales aplicables a las empresas y unidades de la Secretaría de Educación y Cultura del Tolima en materia de seguridad y privacidad de la información con el fin de garantizar el cumplimiento de estos.
- Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales.
- Establecer los lineamientos mínimos requeridos para garantizar una adecuada administración y protección de la información contenida en las bases de datos, así como de la determinación de las estrategias para la protección de datos personales.
- Monitorear y hacer seguimiento a la normatividad expedida en materia de protección de la información y hacer recomendaciones de ajustes al interior de la Secretaría de Educación y Cultura del Tolima.
- Actuar como coordinador con las demás áreas que conforman la Secretaría de Educación y Cultura del Tolima para asegurar una implementación transversal del Programa Integral de Gestión de Datos Personales.
- Conservar un inventario de las bases de datos personales en poder de la Secretaría de Educación y Cultura del Tolima.
- Solicitar ante la Superintendencia de Industria y Comercio las declaraciones de conformidad cuando esto sea requerido.
- Realizar el entrenamiento necesario a los nuevos empleados (inducción), que tengan acceso por las condiciones de su empleo, a datos personales gestionados por la organización.
- Integrar las políticas de datos dentro de las actividades de las demás áreas de la organización (talento humano, seguridad, y gestión de proveedores, etc.).

- Atender las consultas e inquietudes relacionadas con el tratamiento de información personal que titulares, funcionarios y personas o entidades con los que se comparte la información puedan manifestar.
- Mantener documentación actualizada de los procedimientos usados por la Secretaría de Educación y Cultura del Tolima para la recolección, almacenamiento, uso, circulación y supresión de información.
- Valorar los incidentes de seguridad de la información relacionados con información personal con el fin de establecer las medidas correctivas que ameriten y su posterior comunicación a la Superintendencia de Industria y Comercio y los titulares, en caso de considerarlo necesario.
- Adelantar los análisis correspondientes a la manera como se manejan los datos personales por parte de la empresa y proponer el marco metodológico más apropiado para la administración de riesgos.
- Impartir directrices para el relacionamiento con terceros encargados del tratamiento de datos personales, medir la participación y calificar el desempeño de los empleados en materia de protección de datos personales.
- Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice la Superintendencia de Industria y Comercio.
- Registrar las bases de datos de la organización en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la Superintendencia de Industria y Comercio.

Contacto con las autoridades

- Garantizar la creación y actualización del listado de contactos de las autoridades relacionadas con la Seguridad y Privacidad de la información.
- Definir y comunicar un procedimiento a través del cual se especifique el motivo, el medio y la autoridad a quien se debe comunicar los incidentes relacionadas con la Seguridad y Privacidad de la información.

Contacto con los grupos de interés

- Garantizar la creación y actualización del listado de contactos con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad y privacidad de la información.

2.14. Política De Gestión De Almacenamiento

Objetivo: Proteger la información de la Secretaría de Educación y Cultura del Tolima - SEDTOLIMA velando por la protección de la confidencialidad, integridad y disponibilidad de la información que se encuentra en unidades de almacenamiento.

Políticas:

- Todos los funcionarios y/o contratistas de la entidad deberán salvaguardar su información en la herramienta ONEDRIVE.

- La oficina de GETICSI, no realizará copias de seguridad de información de usuarios, al momento de cambio de equipos ya sea por daño o reposición del mismo, la información del funcionario deberá tenerla en ONEDRIVE para su sincronización.

- Se restringe el uso de carpetas compartidas desde equipos de escritorio. Si el funcionario y/o contratista no adopta esta política la Oficina de Gestión de Tecnología y Sistemas de Información (GETICSI) de la SEDTOLIMA no se hace responsable de la pérdida o infiltración de la información.

- Las carpetas compartidas sobre la infraestructura ofrecida por GETICSI como SharePoint, OneDrive, serán administradas por las áreas quienes velarán por el buen uso de la información y de las carpetas.

- Se debe documentar los permisos y accesos sobre la carpeta compartida, usando los siguientes criterios:
  - Permisos de Lectura
  - Permisos de Escritura y modificación
  - Permisos de Control Total.

  Lo cuales serán documentados por el área de GETICSI, A través del Macroproceso L. Gestión de la tecnología informática

- La información CLASIFICADA, RESERVADA O PUBLICA de las áreas de la institución debe utilizarse las carpetas destinadas en el OneDrive y no podrá borrarse en ningún momento.

- Se prohíbe el acceso a carpetas compartidas a usuarios que no tengan una vinculación directa con la SEDTOLIMA o con la GOBERNACION DEL TOLIMA.

- Se prohíbe la publicación de archivo ejecutables (.exe, bat y dll entre otros) en las carpetas compartidas de Onedrive, SharePoint, si el área requiere usar alguna de las extensiones mencionadas, debe justificarlo a la oficina de GETICSI para ajustar la política, como se defina según acuerdo por las dos áreas.

- Se prohíbe el uso carpetas para el almacenamiento de archivos personales, música, videos, imágenes y cualquier otro tipo de archivo no relacionados con el cumplimiento de la función del colaborador.

- La oficina de GETICSI define que los nombres a los archivos y carpetas sean lo suficientemente significativo sin que sea demasiado extenso, y que no contengan nombres de los usuarios. Se establece como longitud máxima para un nombre de archivo, 256 caracteres (un carácter puede ser una letra, número o un símbolo).

- El único medio de respaldo de la información para los funcionarios de la sedtolima es OneDrive, el cual será configurado por la Oficina de GETICSI, la configuración de la herramienta deberá solicitarla al correo gestion.tecnologia@sedtolima.gov.co.

- La oficina de GETICSI no se hace responsable por información que no se encuentre salvaguardada en dicha herramienta

Gestión y Disposición de medios removibles

- Todos los dispositivos y unidades de almacenamiento removibles, tales como cintas, CD's, DVD's, dispositivos personales "USB", discos duros externos, cámaras fotográficas, cámaras de video, celulares, entre otros, deben ser controlados desde su acceso a la red de la SEDTOLIMA y uso hasta finalización de su contrato o cese de actividades.

- Toda la información clasificada como CONFIDENCIAL o RESERVADA que sea almacenada los diferentes activos de información que se requiera de protección especial de acuerdo con la calificación otorgada en el levantamiento de activos de información, debe cumplir con las directrices de seguridad estipuladas para la protección de los mismo.

- Se debe llevar el registro de todos los medios removibles de la SEDTOLIMA y mantenerlo actualizado.

- Todos los medios removibles deben ser almacenados de manera segura.

- El Oficina de GETICSI puede restringir que medios de almacenamiento removibles se conecten a los equipos de cómputo que sean propiedad de la SEDTOLIMA o que estén bajo su custodia, y puede llevar a cabo cualquier acción de registro o restricción, con el fin de evitar fuga de información a través de medios removibles.

- Los medios de almacenamiento removibles que se conecten a la red de datos de la SEDTOLIMA o que se encuentren bajo su custodia, están sujetos a monitoreo por parte del Oficina de GETICSI.

- Todos los retiros de medios de almacenamiento de las instalaciones de la SEDTOLIMA, como discos duros externos, se deben realizar con la autorización del propietario del proceso misional, estratégico, mejora continua o de apoyo, definidos de acuerdo al mapa de procesos de la SEDTOLIMA, a través del formato orden de salida de elementos.

- Todos los medios de almacenamiento removibles propiedad de la SEDTOLIMA, deben estar almacenados en un ambiente seguro acorde con las especificaciones del fabricante.

- Se debe hacer seguimiento a los medios de almacenamiento removibles como Discos Duros, Cintas, etc, con el fin de garantizar que la información sea transferida a otro medio antes de que esta quede inaccesible por deterioro o el desgaste que sufren a causa de su vida útil.

Borrado seguro

- Todos los medios de almacenamiento que sean de propiedad de terceros y que sean autorizados por la SEDTOLIMA para su uso dentro de la red corporativa, deben contar con su respectivo soporte.

- Todos los medios de almacenamiento que contengan información de la SEDTOLIMA y que salgan de la Entidad y que no se les vaya a dar más uso, deben seguir el procedimiento de borrado seguro definido por la SEDTOLIMA, el cual garantiza que la información no es recuperable (Aplica para medios de almacenamiento de equipos alquilados, equipos para pruebas de concepto, equipos de proveedores, discos duros externos, etc.).

- Los medios de almacenamiento que contengan información de la SEDTOLIMA y que vayan a ser dados de baja o reutilizados, deben seguir el procedimiento de borrado seguro definido por la SEDTOLIMA, el cual garantiza que la información no se es recuperable (Aplica para medios de almacenamiento externos o de equipos que son

reasignados, formateados, reinstalados o que por degaste o falla son retirados o dados de baja).

- Eliminar de forma segura (destrucción o borrado) los medios de almacenamiento que no se utilicen y que contengan información de la SEDTOLIMA.

Trasferencia de medios físicos

- Toda la información clasificada como CONFIDENCIAL o RESERVADA que se desee almacenar en medios removibles y que sean transportados fuera de las instalaciones de la SEDTOLIMA, debe cumplir con las disposiciones de seguridad indicadas por la Oficina de GETICSI, específicamente aquellas referentes al empleo de técnicas de cifrado.

- El transporte de los medios físicos se debe hacer mediante un medio de transporte confiable y seguro, tomando las medidas y precauciones necesarias para garantizar que los medios de almacenamiento sean transportados adecuadamente, de esta forma se evitar una afectación a la integridad y disponibilidad.

- Se debe llevar un registro o cadena de custodia de los medios de almacenamiento físico que son transportados.

5. IDENTIFICACION DE CAMBIOS

FECHA		VERSIÓN
Noviembre de 2020	• Se define el manual de Políticas Complementarias de Seguridad y Privacidad de la Información	01
Diciembre de 2021	• Se incluye la política 2.14 Política De Gestión De Almacenamiento	02