DISEÑO DE UN MODELO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE TALENTO HUMANO DE LA SECRETARÍA DE EDUCACIÓN

TRABAJO DE GRADO

EMILIO ANTONIO SANCHEZ PACHECO
Código 1612010776

FAVER LISANDRO REBOLLEDO HINOJOSA
Código 1522010622

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2017

DISEÑO DE UN MODELO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE TALENTO HUMANO DE LA SECRETARÍA DE EDUCACIÓN

TRABAJO DE GRADO

EMILIO ANTONIO SANCHEZ PACHECO
Código 1612010776

FAVER LISANDRO REBOLLEDO HINOJOSA
Código 1522010622

Asesor
ALEJANDRO CASTIBLANCO CARO
Coordinador Investigación y Posgrados

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2017

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firmas de los jurados

Arauca, 17 de Septiembre de 2017

TABLA DE CONTENIDO

INTRODUCCIÓN

Unos de los desafíos que posee cada una de las entidades públicas es asegurar y proteger los datos y documentos con que cuentan los funcionarios en sus áreas de trabajo para su labor cotidiana, por esto se debe recurrir a buenas estrategias para contrarrestar los peligros que puedan existir contra toda información que se produzca en ellas.

Se hace de mucha importancia establecer un sistema estructurado que gestione la seguridad de activos en las entidades públicas, consiguiendo con esto identificar con más rapidez los riesgos que puedan causar perjuicio y la prevención que pueda realizar por parte de los dirigentes sobre la problemática identificada, evitando que haya fuga y daño de sus activos de información.

Las entidades del sector público de Colombia para dar acatamiento a las normatividades en protección y privacidad de datos almacenados deben construir niveles de seguridad muy importantes para no tener que verse envueltos en demandas por parte de los ciudadanos.

Por lo tanto al diseñar un modelo que gestione la seguridad de información en empresas púbicas con el modelo de seguridad y privacidad de la información del ministerio de las tecnologías y comunicaciones, y ponerlo en práctica conlleva a poder obtener la certificación y crear una imagen de prestigio y de interés a la comunidad, contribuyendo ampliamente a la transparencia en gestión pública y seguridad digital.

Para la culminación de la especialización se expone el siguiente trabajo enfocado en el diseño de un modelo de gestión de seguridad de la información en el área de talento humano de la secretaría de educación para lograr la finalidad de mantener ante todo la protección y control de la información que se produce en dicha área durante todo su ciclo de vida, basado en el modelo de seguridad y privacidad de la información de la estrategia de gobierno en línea. [1]

El desafío es lograr que el modelo planteado conduzca a una solución eficaz y eficiente, que emita los niveles de seguridad requeridos y brinde la confianza necesaria en directivos y funcionarios de la entidad.

AGRADECIMIENTOS

Damos gracias primordialmente a Dios por bendecirnos cada, porque nos ha dado inteligencia, sabiduría, paciencia, entendimiento, dedicación y la capacidad para ejercer este proyecto de grado de la mejor manera.

A los licenciados e ingenieros de esta especialización, por transferir sus conocimientos sobre seguridad de la información, de sus disposiciones y aportes para nuestro aprendizaje

Al Ing. Diego Alejandro Corrales Caro, en su carácter de revisor en la primera etapa de este proyecto, por su buena disposición, aportes y comentarios al mismo.

Al Ing. Alejandro Castiblanco Caro, en su carácter de revisor en la entrega final de este proyecto, por su buena disposición, aportes y comentarios al mismo.

A todos los familiares, amigos y personas cercanas, por darnos ese aliento positivo para la culminación de ciclo más de nuestras vidas.

1. RESUMEN EJECUTIVO

La secretaría es una empresa estatal manejada por el ente territorial del departamento, gobernación, esta secretaría se encarga de los procesos de la cobertura educativa, la calidad educativa, inspección y vigilancia de los establecimientos educativos, administrativa y financiera, Jurídica, sistema de atención al ciudadano y talento humano, articulado en un conjunto de procesos para el buen funcionamiento de los establecimientos educativos y del recurso humano como son los profesores, administrativos y sobre la buena educación para los jóvenes del departamento.

En la secretaría de educación departamental no se tiene una política de seguridad definida, no existen mecanismos o procedimientos establecidos para la administración apropiada y segura de los activos de información, por lo tanto se han presentado riesgos como:

- De seguridad, por perdida de documentos e información necesarias para el buen desarrollo de la organización en cada una de las áreas de la secretaría.
- Se detectan riesgos de seguridad y acceso por el mal manejo de las claves para entrar a los sistemas de información, éstas son débiles y la prestan para que otros funcionarios entren con sus usuarios sin cambiarlas nuevamente.
- También se detectan riesgos por disponibilidad, por pérdida y daño de expedientes laborales de los profesores y administrativos.
- La mayor causa de las vulnerabilidades y riesgos se da por el uso incorrecto de la tecnología.
- Integridad del software y la información, por la instalación de software sin autorización del área de sistemas o el coordinador de IT.
- De infraestructura, por falta de protección de los equipos de cómputo por altos voltajes de corriente.
- Navegación por páginas web que no tienen que ver con el trabajo del funcionario.
- Seguridad y acceso por equipos de cómputos conectados a la red sin ser autorizados.
- Integridad y disponibilidad por no haber herramientas y equipos para realizar backup periódicamente de la información.

Según lo expuesto, la Secretaría de Educación Departamental requiere implementar unos controles y medidas para mitigar los riegos de pérdida parcial o total de información valiosa para el buen funcionamiento de ella, con el objetivo de mantener la integridad, confidencialidad y disponibilidad de la información.

De acuerdo a lo anterior, se puede establecer que la problemática está relacionado con que la secretaría no cuenta con un modelo de seguridad de la información, y por lo tanto se necesita en este momento el diseño de un sistema de gestión de seguridad de la información, el cual estaría basado en un estándar de primera categoría, con el propósito que sea factible la generación de las actividades que se tengan que realizar.

Por lo tanto el grupo de trabajo propuso el objetivo general como el diseñar un modelo de gestión de la seguridad de la información en el área de talento humano de la secretaría de educación con el fin de mantener la Confidencialidad, Integridad, Disponibilidad y Control de la información que se produce en dicha área durante todo su ciclo de vida, basado en el modelo de seguridad y privacidad de la información de la estrategia de gobierno en línea.

Para lograr este objetivo general se propusieron los siguientes objetivos específicos:

- Definir la política general y específica, alcance y objetivos del Sistema de Gestión de Seguridad de la información.
- Definir y seguir una metodología de riesgos de seguridad de la información donde se identificaran los criterios necesarios para identificar las amenazas que pueden materializar como riesgo contra los activos de información.
- Diseñar un plan de trabajo donde se relacione actividades de concienciación sobre los riesgos y seguridad de la información para el personal administrativo del área de talento humano de la secretaría.
- Diseñar un plan de trabajo para la digitalización de todos los expedientes de la Secretaría.

Se espera por parte de este trabajo la culminación de los objetivos específicos con la creación de los cuatro entregables al final de este proyecto, que son:

- Política y objetivos de seguridad de la información.
- Metodología de Riesgos de Seguridad de la Información.
- Plan de trabajo de concienciación de seguridad de la información.
- Plan de trabajo para la digitalización de todos los expedientes.

La guía metodológica para el desarrollo de los dos primeros entregables se desarrollará en base al modelo de seguridad y privacidad de la información de la estrategia de gobierno en línea, el cual está alineado a la norma internacional 27001 del 2013, y del cual se utilizaran la guía 2 política general MSPI, la guía 5 gestión clasificación de activos y la guía 7 que es la gestión de riesgos. Para el entregable plan de trabajo de concienciación de seguridad de la información se diseñará por medio de información que se pueda conseguir en internet sobre el tema y las normas existentes sobre SGSI; y para el último entregable plan de trabajo para la digitalización de todos los expedientes, se diseñará con información suministrada por la entidad y propia de los autores.

El resultado final obtenido por el grupo de trabajo fue la realización del proyecto con sus entregables tales como:

Política y objetivos de seguridad de la información, el cual se divide en cinco partes: la política general y específica de seguridad de la información, alcance y aplicabilidad, nivel de cumplimiento, las políticas específicas, y los objetivos de la seguridad de la información; logrando con esto una política enmarcada en el funcionamiento de la entidad, como son sus objetivos institucionales y proceso misional del área de talento humano; logrando al final que fuera concisa, fácil de leer y de entender por todos los funcionarios del alcance de la política.

Metodología de Riesgos de Seguridad de la Información, se realizó primero que todo la metodología o pasos a seguir para el área de talento humano de acuerdo al modelo de seguridad y privacidad de la información de la estrategia de gobierno en línea, luego se realizó la gestión y clasificación de los activos de información, identificación y valoración de las amenazas y por último el análisis de riesgo, teniendo como resultado las acciones de mitigaciones o controles que implantados por la entidad buscaran reducir el riesgo de disponibilidad, confidencialidad e integridad en los activos de la información seleccionados de la secretaría de educación del área talento humano.

Plan de trabajo de concienciación de seguridad de la información, en el proceso se realizaron los objetivos del plan de concienciación, a quienes iba destinado el plan, las actividades a desarrollar, el cronograma de actividades, y por último el seguimiento al plan, logrando con esto una buena construcción de este entregable el cual podrá orientar a la entidad en temas de seguridad y que todos los funcionarios se capaciten y se comprometan a tener mucho cuidado con la información que manejan en sus puestos de trabajo.

Plan de trabajo para la digitalización de todos los expedientes, se concluye con la creación del plan de trabajo para que la entidad pueda cumplir con toda la digitalización de los expedientes de todos sus trabajadores, dando cumplimiento al resguardo digital de toda la información que se encuentra físicamente y que en algún momento se pueda deteriorar con el tiempo por eventualidades externas o internas a la secretaría.

El alcance del proyecto abarca el diseño del modelo de Gestión de Seguridad de la información en el área de talento humano de la secretaría de educación, cubriendo la primera fase de la implementación de un SGSI correspondiente a la etapa de planeación. Abarca únicamente el Proceso del área de talento humano de la secretaría de educación, en el cual se clasificaran los activos de información y valoración de riesgos solo para este proceso y la política general.

Para el desarrollo del proyecto se utilizará la guía del SGSI del Ministerio de las TIC, basado en el modelo de seguridad y privacidad de la información de la estrategia de gobierno en línea y la norma internacional 27001 de 2013. De este MSPI se trabajará con la Guía 2, Política General MSPI v1, la Guía 5, Gestión clasificación de activos y la Guía 7, Gestión de riesgos.

2. JUSTIFICACIÓN

Basándose en el modelo de seguridad y privacidad de la información de la estrategia de gobierno en línea (MSPI GEL), el cual está basado en las buenas prácticas de seguridad de la norma internacional ISO 27001 2013, proporcionará seguridad en la información mediante la protección de sus activos, con el fin de cumplir las políticas y objetivos estratégicos de la secretaría de educación, y así garantizando un buen servicio por parte de la secretaría de educación con respecto a la comunidad educativa.

Un SGSI busca que los funcionarios de la entidad fortalezcan íntegramente los pilares fundamentales de la seguridad como son la integridad, confidencialidad y disponibilidad de la información, como también ayudando a crear cultura apropiada de proteger la información.

Estableciendo el SGSI puede traer varias ventajas para la entidad, como pueden ser: el compromiso de la secretaría que tiene con respecto a la seguridad de la información, poder determinar y construir mecanismos para gestionar de una manera más fácil y pronta los riesgos tantos físicos como lógicos que puedan afectar la información, generar crecimiento en la imagen de la entidad en el sector de la educación, y con todas estas ventajas se podrá brindar una información de calidad a la comunidad educativa y poder cumplir los siguientes objetivos de seguridad:

- Promover la cultura de Seguridad de la Información en cada uno de los funcionarios de la secretaría de educación, facilitando la tarea de proteger los activos de información.
- Crear en el trabajador de la secretaría de educación sentido de pertenencia y apropiación en los temas de seguridad, con el fin de proteger la información de la entidad de ataques externos e internos.
- Concientizar a los funcionarios de la Secretaría con relación a los riesgos que pueden afectar la protección de la información en sus tres pilares, la integridad, confidencialidad y disponibilidad.
- Buscar mecanismos para que los funcionarios pongan en ejercicio las políticas, procedimientos y las buenas prácticas de seguridad definidas por los directivos de la entidad, comprendiendo a su vez las implicaciones, peligros y riesgos de sus acciones en contra de los activos de la secretaría.
- Gestionar los riesgos que puedan causar daño a la información.
- Realizar mejoras continuas del sistema de gestión de seguridad de la información.

- Promover cultura de seguridad al interior de la entidad, entre ellas la información que se debe proteger para así tener inversiones mínimas en seguridad y tecnología. [1]

Diseñando y desarrollando un MSI en la entidad ayudará a mejorar el cumplimiento de los indicadores establecidos en la problemática encontrada.

Indicador: Capacitación en Seguridad de la Información en usuarios de estaciones de trabajo.
En que puede ayudar el modelo de seguridad de la información:

- Impulsar el conocimiento sobre seguridad de la información internamente en la secretaría, capacitando los funcionarios en temas de buenas prácticas de seguridad.
- Proveer procesos que fomenten en los trabajadores concienciación con relación a la seguridad, evitando con esto que se pierda o se destruya la información.
- Orientar en los empleados de la secretaría un lenguaje común sobre la protección de la información.
- Ampliar en los funcionarios las mejores prácticas y los buenos hábitos en seguridad de la información.
- Creando al interior de la organización una buena cultura de seguridad de los activos de información, dejando en claro cuál es la información que se debe proteger, evitando inversiones innecesarias en seguridad y tecnología.[2]

Indicador: Copias de Seguridad y Digitalización de Expedientes
En que puede ayudar el modelo de seguridad de la información:

- Establecer una buena política específica y darla a conocer al personal encargado en este proceso evita que haya pérdida de información en la secretaria.

Indicador: Pérdida o modificación de Información
En que puede ayudar el modelo de seguridad de la información:

- Generando en los empleados de la secretaría sentido de pertenencia y apropiación en cuanto a la seguridad de los activos de información, logrando una participación activa de toda la secretaría en la planeación, definición, identificación de riesgos e implementación de controles y medidas orientadas a proteger la información, evitando con ello la pérdida o modificación de ésta.[3]

[1] Carlos Alberto Guzmán Silva. Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso. http://repository.poligran.edu.co/. Pág. 26-27
[2] Ibíd., Pág. 28
[3] Ibíd., Pág. 27

3. MARCO TEÓRICO Y REFERENTES

3.1 MARCO TEÓRICO

En el trayecto de la vida se ha buscado la seguridad permanente de la información o activos con que cuentan las organizaciones, para cumplir con este objetivo se han desarrollado normas o estándares que con el transcurso de la era digital se han perfeccionado con el fin que las empresas pongan en práctica ciertos criterios para contrarrestar la cantidad de amenazas que surgen todos los días en contra la información y activos.

Para lograr el propósito de la seguridad de la información en las entidades de mantener seguro los activos de información de debe contar con una metodología que detecte con anticipación los riesgos que pueden tener ciertas amenazas contra ellos.

El objetivo primordial de la metodología de valoración y tratamiento de riesgos de seguridad es conocer el estado real de seguridad con que cuenta la empresa, tanto física como lógicamente, y si es posible determinar medidas de seguridad para lograr minimizar el riesgos que pueden llevar al no cumplimiento de la actividad de la organización.

En sí, el sistema de gestión de seguridad, es un conjunto específico de seguridad física y lógica que deben llevar las empresas para dar cumplimientos a normatividades y seguridad de sus activos con el propósito de cumplir sus metas y objetivos.

Para efecto del presente trabajo se darán claridad a ciertos conceptos que tienen que ver con la seguridad de la información en las organizaciones.

3.1.1 SEGURIDAD DE LA INFORMACIÓN

La Seguridad de la Información, según ISO 27001 [2], se refiere a la confidencialidad, la integridad y la disponibilidad de la información importante para la organización, independientemente del formato que tengan, estos pueden ser: electrónicos, en papel, audio y vídeo, etc.

También se puede definir que el objetivo de la seguridad de la información es asegurar que los recursos que cuenta la empresa sean utilizados de la forma como se encuentre estipulada en la organización, así como controlar que la modificación

solo sea posible por parte de las personas autorizadas para tal fin y por supuesto, siempre dentro de los límites de la autorización.

La participación en seguridad de la información debe ser constante por todos los funcionarios de una organización con el fin de poder preservar la confidencialidad, la integridad, la disponibilidad, autenticidad y trazabilidad, entre otros principios

3.1.2 GESTION DE SEGURIDAD DE LA INFORMACION [3]

Es un proceso que las organizaciones deben llevar con respecto a las amenazas que puedan existir contra sus activos de información y que se puedan materializar como riesgos de consideración.

La única manera de manejar un porcentaje mayor de las medidas de seguridad será establecer los procesos de seguridad y determinar las responsabilidades, esto sería un enfoque basado en procesos dentro de los estándares de gestión según la norma ISO 27001.

Para saber que los controles de aseguramientos de la información trabajen para lo que fueron contratados se debe tener un enfoque bien claro sobre quien cae la responsabilidad de sus funcionamientos y que se debe hacer si alguno de ellos pueda fallar en un momento cualquiera.

Debemos tener en cuenta que los controles de seguridad de la información no son sólo técnicas implementadas, son controles que deben estar relacionados con la tecnología de la información. Se pueden tener diferentes tipos de controles, por ejemplo la documentación de un procedimiento es un control de la organización, la implantación de una herramienta de software será un control de tecnología de la información y la formación de funcionarios es un control de recursos humanos.

Al construir un sistema de gestión de seguridad de la información se describen un conjunto de reglas de seguridad de la información, quienes pueden ser los responsables de la seguridad y que controles se pueden adaptar para proteger la información, y así la seguridad no se convertiría en algo inmanejable.

Entonces podemos concluir que el SGSI es un conjunto de procesos relacionados entre sí que tienen la finalidad de brindar seguridad a los activos de la empresa.[4]

[4] https://www.isotools.org/2016/07/07/sistema-gestion-seguridad-la-informacion-basado-la-norma-iso-27001/

3.1.3 SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION [4]

Sus siglas son SGSI y se puede concluir que es un conjunto de técnicas y actividades que tienen como objetivo velar por la confidencialidad, integridad y disponibilidad de la información.

El modelo de gestión de la seguridad tiene como objeto planificar y crear procedimientos adecuados, para luego implementar controles de seguridad basados en una evaluación de riesgos y consiguiendo mediciones de eficiencia de los mismos.

Al establecer las políticas de seguridad y los procedimientos en relación a los objetivos del negocio de la empresa, y tener como objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir, se empieza a hablar de un SGSI.

Entre los beneficios que puede otorgar un SGSI se tienen:

- Establece una metodología estructurada para la gestión de seguridad.
- Se puede reducir el riesgo pérdida de la información importante de la organización.
- Hay acceso a la información por parte del cliente con medidas de seguridad.
- Se revisan periódicamente los riesgos y los controles que se apliquen.
- Hay confianza de los clientes y los socios de la empresa.
- Se realizan auditorías externas para ayudar a identificar las debilidades del SGSI encontrando que áreas se deben mejorar.
- Se facilita la integración con otros sistemas de gestión.
- Se garantiza la continuidad de negocio tras incidentes graves.
- Cumplimiento con la legislación vigente sobre información personal, propiedad intelectual y demás.
- Mejora la imagen de la organización a nivel nacional o internacional.
- Se producen reglas claras para los funcionarios de la empresa.
- Reduce los costos y mejoras de los procesos y el servicio.
- Produce motivación y satisfacción del personal de la organización
- Aumenta la seguridad en base la gestión de procesos en vez de compras sistemáticas de productos y tecnologías.[5]

[5] SGSI - Blog especializado en Sistemas de Gestión de Seguridad de la Información. http://www.pmg-ssi.com/2015/07/que-es-sgsi/

3.1.4 MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI) DEL MINTIC [1]

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; publica El Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL:TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

Según el MINTIC este MSPI se actualiza periódicamente según la normativa 27001, la ley de protección de datos personales, transparencia y acceso a la información pública, con el fin de estar acorde con todas estas legislaciones en gestión de la información

A nivel metodológico cuenta con varias guías anexas que ayudaran a las entidad seguir detalladamente las fases del modelo, y poder comprender a su vez los resultados obtenidos por cada etapa desarrollada.

El MINTIC desarrolla este modelo para que las entidades del estado tengan una guía, contribuyendo transparencia en gestión pública, y promoviendo el uso de las mejores prácticas de protección de la información.

Sus anexos son:

- Guía 1 - Metodología de pruebas de efectividad
- Guía 2 - Política General MSPI v1
- Guía 3 - Procedimiento de Seguridad de la Información
- Guía 4 - Roles y responsabilidades
- Guía 5 - Gestión Clasificación de Activos
- Guía 6 - Gestión Documental
- Guía 7 - Gestión de Riesgos
- Guía 8 - Controles de Seguridad de la Información
- Guía 9 - Indicadores Gestión de Seguridad de la Información
- Guía 10 - Continuidad de Negocio
- Guía 11 - Análisis de Impacto de Negocio
- Guía 12 - Seguridad en la Nube
- Guía 13 - Evidencia Digital (En actualización)
- Guía 14 - Plan de comunicación, sensibilización, capacitación
- Guía 15 - Auditoria
- Guía 16 - Evaluación de Desempeño
- Guía 17 - Mejora continua

- Guía 18 - Lineamientos terminales de áreas financieras de entidades públicas
- Guía 19 - Aseguramiento de protocolo IPv4_IPv6
- Guía 20 - Transición IPv4_IPv6
- Guía 21 - Gestión de Incidentes
- Modelo de Seguridad y Privacidad[6]

3.1.5 NORMAS FAMILIA ISO/IEC 27000 [2]

La norma internacional ISO 27000 se compone de una serie de estándares desarrollados, hay otras que todavía están en desarrollo, por la International Organization for Standardization e International Electrotechnical Commission, todo este conjunto de normas proporcionan un marco de gestión de la seguridad de la información y cualquier organización o empresa las pueden utilizar.[7]

El organismo encargado de normalizar este tipo de normas en Colombia es el ICONTEC (Instituto Colombiano de Normas Técnicas y Certificaciones).

A continuación se darán a conocer algunas normas de ISO/IEC 27000.

ISO/IEC 27000: Es la norma que general que recoge todas las definiciones sobre las normas que la componen, donde indica el alcance y propósito de cada una de ellas, también se encuentran descripciones y conceptos sobre el SGSI. Fue publicada el 01/05/2009 y tiene su última versión el 14/01/2014.[8]

ISO/IEC 27001: Esta es la norma primordial de todas en la serie y contiene todos los requisitos de SGSI, compuesta por el Anexo A, donde se enumera resumida los objetivos de control y controles a desarrollar en la norma ISO 27002. Se publica el 15 de octubre de 2005, y su última revisión el 25 de septiembre de 2013 y es certificable.[9]

ISO/IEC 27002: Esta norma es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en la seguridad de la información, Contiene 39 objetivos de control y 133 controles agrupados en dominios. Nace el primero de julio de 2007 y no es certificable.[10]

ISO/IEC 27003: Esta norma es la guía que se concentra en los detalles críticos que se necesitan para el diseño e implementación de un SGSI para que sea

[6] Modelo de Seguridad en http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html
[7] El portal del ISO 27001 en español en http://www.iso27000.es/iso27000.html
[8] Ibíd., ISO/IEC 27000
[9] Ibíd., ISO/IEC 27001.
[10] Ibíd., ISO/IEC 27002.

exitoso. Esta norma se dio a conocer el primero de febrero de 2010 la cual no es certificable.[11]

ISO/IEC 27004: Esta norma se creó para utilizar procedimientos de medidas que pueden determinar la eficacia del SGSI y de todos los controles implementados. Publicada el 15 de diciembre de 2009.[12]

ISO/IEC 27005: Esta norma proporciona criterios para la gestión del riesgo en la seguridad de la información de las organizaciones. Publicada el primero de junio de 2011 y no es certificable.[13]

ISO/IEC 27006: La norma específica los requisitos para la acreditación de entidades de auditorías y certificación de SGSI. Fue dada a conocer el primero de diciembre de 2011 y no es certificable.[14]

ISO/IEC 27035: La norma proporciona una guía sobre la gestión de incidentes de seguridad de la información. Se dio a conocer el 17 de agosto de 2011.

Y otras más que se encuentran en el portal de ISO 2700 en español [2] y su referencia de búsqueda se encuentra en el apartado de la bibliografía.

3.1.6 CICLO DE MEJORA CONTINÚA EN LA NORMA ISO/IEC 27001:2013

Para la ISO/IEC 27001:2013 se basa en el ciclo de mejora continua o Deming (Plan, Do, Check, Act).[15]

Las fases PHVA con la estructura ISO 27001:2013:

- Fase Planear: Están los del contexto de la organización, liderazgo, planificación y soporte.
- Fase Hacer: Está la operación.
- Fase Verificar: Está la evaluación de desempeño
- Fase Actuar: Se encuentra la mejora.

Planificar o planear: En esta fase se realiza el establecimiento del SGSI, Se establecen: políticas, objetivos, alcance, análisis de riesgo, controles de seguridad.

[11] Ibíd., ISO/IEC 27003.
[12] Ibíd., ISO/IEC 27004.
[13] Ibíd., ISO/IEC 27005.
[14] Ibíd., ISO/IEC 27006.
[15] ISO/IEC 27001:2013 - Ciclo de mejora continua o Deming en http://seguridadinfoperu.blogspot.com.co/2017/05/isoiec-270012013-ciclo-de-mejora.html

Hacer: En esta fase se implementa y opera el SGSI, Tiene como objeto fundamental garantizar una adecuada implementación de los controles seleccionados y la correcta aplicación de los mismos.

Verificar: En esta fase se revisa y se da seguimiento al SGSI, realizando auditorías y revisando los indicadores.

Actuar: En esta fase de mantiene y se mejora el SGSI, realizando acciones correctivas y acciones preventivas, para lograr la mejora del SGSI.

3.2 MARCO CONCEPTUAL

En este apartado se tendrán una colección de definición de términos que se manejan en el SGSI.

Activo de información: Es la información importante para las empresas y pueden estar conformados por: bases de datos, ficheros, contratos, acuerdos, registros del sistema, aplicaciones, manuales, procedimientos, software, entre otros.

Amenaza: hecho que puede producir un daño a los activos provocado por un evento.

Análisis de riesgos: Procesos que se llevan a cabo para identificar las amenazas que pueden tener los activos de información y procurar minimizar si se materializan en riesgos.

Causa: Es el motivo por la cual sucede algo.

Ciclo de Deming: Es conocido como círculo PDCA (plan-do-check-act, significa, planificar-hacer-verificar-actuar) o espiral de mejora continúa, es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart.[16]

Confidencialidad: Propiedad que garantiza la accesibilidad de la información únicamente al personal autorizado.[17]

Controles: Mecanismos físico o lógicos que se utilizan para monitorear y controlar acciones dentro de una empresa.[18]

[16] Círculo de Deming en https://es.wikipedia.org/wiki/C%C3%ADrculo_de_Deming
[17] Confidencialidad en https://es.wikipedia.org/wiki/Confidencialidad
[18] Controles de seguridad y privacidad de la información

Disponibilidad: Propiedad que garantiza que la información se pueda acceder y utilizar por las personas que están debidamente autorizadas.[19]

Impacto: Es el resultado obtenido a partir de la materialización de una amenaza.[20]

Integridad: Propiedad que garantiza que la información esté exacta y se encuentre completa.[21]

MINTIC: Siglas del Ministerio de las tecnologías y las comunicaciones en Colombia.

MSPI: Es la sigla del Modelo de Seguridad y Privacidad de la Información

Oficial de Seguridad: Es el responsable máximo en planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones con el fin de mejorar la seguridad de la información dentro de sus pilares fundamentales de confidencialidad, integridad y disponibilidad.[22]

Probabilidad de ocurrencia: Estimación de ocurrencia de una evento el cual está relacionado a características de las vulnerabilidades presentadas y el origen de la amenaza.[23]

Riesgo: Grado de exposición de un activo el cual permite la materialización de una amenaza ocasionando daños a la compañía.[24]

Seguridad de la Información: Conjunto de medidas que permiten proteger la información de la empresa.

SI: Sigla de Sistema de Información

SGSI: Es la sigla del Sistema de Gestión de Seguridad de la Información.

Vulnerabilidad: Las vulnerabilidades son puntos débiles existentes que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad de la información.

---

[19] Disponibilidad en https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n
[20] Cartilla introducción teórica al análisis de riesgos. Institución Universitaria Politécnico Grancolombiano
[21] Integridad en https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n
[22] Oficial de seguridad de la información en https://es.wikipedia.org/wiki/Oficial_de_seguridad_de_la_informaci%C3%B3n
[23] Cartilla introducción teórica al análisis de riesgos. Institución Universitaria Politécnico Grancolombiano
[24] Ibíd. Pág. 7

4. METODOLOGÍA

En este apartado se detalla las técnicas utilizadas para alcanzar los objetivos y alcances propuestos al problema que presenta la secretaría de educación con respecto a la seguridad de la información, y así poder cumplir con el propósito con respecto al objetivo general del trabajo.

4.1 TIPO DE INVESTIGACION

EL método de investigación que se aplicará en este proyecto es de tipo factible, el cual consiste en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo para solucionar necesidades organizacionales, donde se puede referir a la formulación de políticas, programas, tecnologías, métodos o procesos[5].

La estructura organizacional del trabajo y algunos conceptos se basaron de publicaciones de temas de especializaciones que se encuentran en repositorios de la Institución Universitaria Politécnico Grancolombiano.[6]

4.2 LINEA DE INVESTIGACIÓN

Se Tomará como referencia el Modelo de Seguridad y Privacidad de la Información (MSPI) de la Estrategia de Gobierno en Línea (GEL), el cual está alineado a la norma NTC-ISO / IEC 27001:2013, por lo cual se puede establecer que la línea de la investigación del proyecto se desarrolla con los temas de tecnología de la información, gestión de la seguridad, gestión de riesgos y sistema de gestión de seguridad de la información.

4.3 INSTRUMENTOS DE RECOLECCION DE INFORMACION

Los mecanismos tenidos en cuenta para el desarrollo de este trabajo fueron la observación directa, documentación existente y evaluación con base en la información recibida en la especialización de seguridad de la información. También fue utilizado diferentes fuentes de información, tales como tesis, blog sobre el tema a tratar, libros, textos, revistas, normas, etc., que se encuentran en formas electrónicas y publicadas en internet.

4.4 FASES METODOLÓGICOS

Para la realización de los entregables se desarrolla en base a el Modelo de Seguridad y Privacidad de la Información (MSPI) de la Estrategia de Gobierno en Línea (GEL), el cual está alineado a la norma NTC-ISO/IEC 27001:2013, los cuales se utilizaron los siguientes anexos o guías del MSPI:

- Guía 2 - Política General MSPI v1
  Política general de seguridad y privacidad de la información.
  Alcance y nivel de cumplimiento.
- Guía 5 - Gestión Clasificación de Activos
  Definición y clasificación de los activos.
- Guía 7 - Gestión de Riesgos
  Identificación y valoración de amenazas.
  Clasificación del riesgo.
  Tabla de probabilidad.
  Tabla de impacto.
  Matriz de clasificación, evaluación y respuesta a los riesgos.
  Gráfico de dispersión o de calor.
  Opciones de tratamiento.
  Acciones de mitigaciones o controles.

Para el entregable plan de trabajo de concienciación de seguridad de la información se diseñará por medio de información que se pueda conseguir en internet sobre el tema, ya que la entidad no cuenta con un sistema de gestión de seguridad de la información.

Para el entregable plan de trabajo para la digitalización de todos los expedientes, se diseñará con información suministrada por la entidad y propia de los autores.

5. RESULTADOS Y DISCUSIÓN

Como se detectó y se identificó la problemática que tiene la secretaría de educación es no contar con mecanismos como políticas, metodologías y planes que generen cultura de seguridad en los funcionarios de esta misma, por lo tanto las actividades realizadas se basó en el eje temático de seguridad y privacidad de la información en el marco de la estrategia de gobierno en línea (MSPI GEL) la cual busca construir un Estado más eficiente, transparente y más participativo gracias a las TIC. Este Modelo de Seguridad y Privacidad de la Información se encuentra alineado al marco de referencia de arquitectura TI y soporta transversalmente a los otros componentes de la estrategia GEL.

Ya que las entidades públicas del estado o territorial están obligadas a implementar esta estrategia las cuales están especificadas en el Decreto Único Reglamentario 1078 de 2015, donde se regula el sector de tecnologías de la información y las comunicaciones. Título 9. Capítulo 1 [7], el grupo de trabajo se alinea a este proceso para dar cumplimiento a los objetivos propuestos en este trabajo.

A continuación se dará explicación detallada de los resultados obtenidos durante el ejercicio del cumplimiento de los objetivos planteados.

5.1 POLÍTICA Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Para el cumplimiento de la definición de la política general, políticas específicas y objetivos de seguridad de la información se siguieron los pasos de la Guía 2 Política General del Modelo de Seguridad de la Privacidad -MSPI-.

Es de suma importancia que la entidad cuente con políticas de seguridad de la información ya que estas guiaran la conducta personal y profesional de todos los funcionarios de la secretaría, haciendo que la entidad trabaje bajo las mejores prácticas de seguridad y cumplimiento de los requisitos legales a los cuales está obligada.

La política general, políticas específicas y objetivos de seguridad de la información se dividieron en cinco partes, las cuales son:

- La política general de seguridad de la información
- El Alcance y aplicabilidad.
- El Nivel de cumplimiento.

- Las políticas específicas.
- Los objetivos de la seguridad de la información.

Teniendo en cuenta la importancia de la entidad, se generó una política donde se tuvo en cuenta el marco general del funcionamiento de ésta, sus objetivos institucionales y proceso misional del área de talento humano, siendo concisa, fácil de leer y de entender, flexible y fácil de hacer cumplir para todos los funcionarios del alcance de la política.

En el Anexo 1 se encuentra el desarrollo del entregable política y objetivos de seguridad de la información.

Como este trabajo tiene como limitante solo realizar el diseño de un modelo de gestión de seguridad en el área de talento humano de la secretaría de educación y no la implementación, por lo tanto se permitió dar alcance al primer objetivo, Definir la política general y específica, alcance y objetivos del Sistema de Gestión de Seguridad de la información, representado en el entregable que se encuentra especificado en el Anexo 1.

5.2 METODOLOGÍA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y SU DESARROLLO

Para el desarrollo de este tema se realizó primero que todo la metodología de acuerdo al modelo de seguridad y privacidad de la información de la estrategia de gobierno en línea (MSPI GEL) del MINTIC, el cual está alineado a la norma internacional ISO 27001:2013, en las guías 5 y 7.

Primero que todo se llevó a cabo los pasos a seguir de la metodología de riesgos de los activos del área de talento humano de la secretaría de educación.

Se realizaron tres pasos para alcanzar el cumplimiento de la metodología:
- Gestión y clasificación de los activos de información
- Identificación y valoración de las amenazas
- Análisis del riesgo

Gestión y clasificación de los activos de información: Se identificaron 4 activos de información:

- ASIN1. Registros completo de nómina
- ASIN2. Información de servidores público
- ASIN3. Expedientes Hojas de Vida
- ASIN 4. Documentación de recobros

Observándose en los resultados, se puede asegurar que los cuatro activos identificados en el área de Talento Humano de la Secretaría, son muy importantes para cumplir con las actividades de los procesos que ejecutan los funcionarios de la entidad y por lo tanto se puede realizar la identificación y valoración de las amenazas que puedan tener estos activos.

Identificación y valoración de las amenazas: Se determinaran los tipos de amenazas y dimensiones para los activos de información (son los datos que serán almacenados en los soportes de información).

Se identificaron tres amenazas por activos, teniendo como resultado un impacto catastrófico, mayor y moderado sobre éstos si llegaran a perder su disponibilidad, integridad o confidencialidad.

Análisis del riesgo: Se realizó la matriz de análisis de riesgo realizado a los activos y amenazas identificados en los puntos anteriores dando como resultado:

- De los 12 riesgos 5 de ellos son de valoración Extremo, para un 41.6%
- 6 de ellos son de valoración Alta, para un 50%.
- 1 de valoración Moderado, para un 8.4%

Y por último se realizaron las acciones de mitigaciones o controles que buscarían mitigar el riesgo de disponibilidad, confidencialidad e integridad en los activos de la información seleccionados en la entidad de la secretaría de educación del área talento humano.

Para la secretaría en el área de talento humano es de mucha importancia el diseño de la metodología de riesgo de los activos de información porque con esto se pueden identificar o gestionar los riesgos que puede tener la información con respecto a sus principios de confidencialidad, integridad y disponibilidad, para así tomar decisiones de como atacar estas brechas de seguridad, ya sea por medio de mitigaciones o controles.

Para que todo el proceso de gestión del riesgo tenga éxito en la entidad se deben identificar tres etapas:

- Compromiso de la alta y media dirección.
- Conformación de un Equipo MECI o de un grupo interdisciplinario.
- Capacitación en la metodología.

Con la realización del entregable metodología de riesgos de seguridad de la información y su desarrollo el cual se encuentra especificado en el Anexo 2, se da el alcance al segundo objetivo de este trabajo, Definir y seguir una metodología de

riesgos de seguridad de la información identificando los criterios necesarios para establecer el nivel de aceptación de impacto para la secretaría

5.3 PLAN DE TRABAJO DE CONCIENCIACIÓN DE SEGURIDAD DE LA INFORMACIÓN

Para la construcción de este plan de concienciación el grupo de trabajo se basó básicamente sobre información que se pudo conseguir en internet sobre el tema.

Los directivos deben tener en cuenta que un plan de concienciación de seguridad en la entidad conlleva a que todos los funcionarios se capaciten y se comprometan a tener mucho cuidado con la información que manejan en sus puestos de trabajo.

En este proceso se realizaron las siguientes etapas para una buena construcción de un plan de trabajo de concienciación:

- Objetivos del plan de concienciación
- Destinatarios del plan de concienciación
- Actividades a desarrollar en el plan de concienciación
- Cronograma de actividades
- Seguimiento del Plan de Trabajo

Se realizaron los objetivos generales del plan, como también los objetivos para cada actividad con el fin de llevar una medición en las tareas que se ejecuten durante el cronograma de actividades.

Como este trabajo se limita al área de talento humano de la secretaría, el plan de concienciación va dirigido al personal antiguo y nuevo que labora en esta área, aunque es muy importante que todo el personal de la entidad sea involucrado en estos planes de concienciación de la seguridad de la información.

Se definieron las actividades a tener en cuenta y con ello se creó el siguiente cronograma de actividades:

Programa	MESES												META (%)
	1	2	3	4	5	6	7	8	9	10	11	12	
Curso Digital				Número de Funcionarios									# Funcionarios 100%

Comunicados periódicos	1	1	1	1	1	1	1	1	1	1	1	1	12 100%
Concurso										1			1 100%
Charlas			1			1			1			1	4 100%

Por último se enunció como va ser el seguimiento de este plan, con el fin de medir el porcentaje de cumplimiento que se lleva del cronograma de actividades.

Según el plan de concienciación de la seguridad de la información que se diseñó y se describe detalladamente en el Anexo 3 se está dando cumplimiento al tercer objetivo específico, Diseñar un plan de trabajo donde se relacione actividades de concienciación sobre los riesgos y protección de la información para el personal administrativo de la sección de talento humano de la secretaría.

5.4 PLAN DE TRABAJO PARA LA DIGITALIZACIÓN DE TODOS LOS EXPEDIENTES

Para la realización de este plan el grupo de trabajo tuvo como fuente principal la información suministrada por la entidad e investigación sobre el tema.

Para realizar el plan se tuvo en cuenta:

- La cantidad de expediente que cuenta la secretaría de educación son de 4.000 y cada uno está conformado por un promedio de 350 folios.
- Los equipos de cómputos y escáner pueden ser prestados por parte de las Instituciones Educativas que son vigiladas por la secretaría y así se ahorraría la compra de estos.
- La revisión de estos equipos se hará por parte del profesional universitario encargado del área de sistemas.
- Adecuación de la oficina con su parte eléctrica y red separada de la secretaría.
- El personal para el escaneo se realizará por medio de alumnos pasantes de una institución local con pensum en ofimática, entre ellas puede ser el SENA
- Compra de discos duros externos y capacitación al personal del subproceso historias laborales.

Con la información dada se calcula el total de recurso humano que se va utilizar para la digitalización, como también la parte tecnológica que se podría utilizar para dicha actividad.

Observando las especificaciones anteriores el plan de trabajo se llevaría de la siguiente manera:

CRONOGRMA PLAN DE TRABAJO				
ITEM	**TIEMPO POR ITEM**			
	1 MES	**2 MES**	**3 MES**	**4 MES**
1. Compra de Discos Duros	X			
2. Búsqueda del personal pasante de una institución local con pensum en ofimática	X			
3. Búsqueda de los equipo de cómputo en los colegios públicos	X			
4. Revisión de equipos por parte del profesional universitario encargado del área de sistemas	X			
5. Adecuación de la oficina con su parte eléctrica y red separada de la secretaría	X			
6. Capacitación al personal		X		
7. 50% de la digitalización de las hojas de vida			X	
8. 50% restante de digitalización de hojas de vida				X

Según hallazgos encontrados por parte de los entes de control, es de suma importancia que las entidades públicas tengan digitalizadas en su totalidad todos los expedientes de sus funcionarios.

Teniendo los expedientes digitalizados le facilita a la entidad con mayor rapidez los tramites que se tengan que realizar con estos activos, y por consiguiente tener una copia digitalizada por si sucede una destrucción total o parcial de éstos por parte de personal ajeno o propio de la secretaría, o por desastres como inundaciones y fuego.

Según el diseño del plan de digitalización de todos los expedientes de la entidad, el cual se describe detalladamente en el Anexo 4 se está dando cumplimiento al cuarto objetivo específico, Diseñar un plan de trabajo para la digitalización de todos los expedientes de la Secretaría.

5.5 RECOMENDACIONES

En el área de talento humano tendrán las funciones de:

- Hacer firmar los acuerdos de confidencialidad a todos los funcionarios nuevos y entrantes.
- Verificar los antecedentes de los funcionarios nuevos a entrar.
- Gestionará para que se lleve a cabo el plan de concienciación diseñado.
- Gestionará para que se cumpla el plan de digitalización de todos los expedientes que reposan en la entidad.
- Gestionará el caso para la baja de los funcionarios que dejen de laborar en la entidad.

El comité directivo tendrá que:

- Revisar y adoptar las políticas y objetivos de seguridad.
- Comprometerse en la conformación de un equipo interdisciplinario de medidas de riesgos de la información.
- Aplicar las acciones de mitigación y controles que se proponen en el desarrollo de la metodología de riesgo.

Evaluar periódicamente el SGSI.

CONCLUSIONES

Lo vital de este trabajo para la secretaría de educación, es que se puede empezar a dar cumplimiento a la implementación de la estrategia de gobierno en línea como entidad pública que está constatada.

El diseño de un Sistema de Gestión de Seguridad de la Información –SGSI- en la secretaría permite descubrir puntos vulnerables de la entidad y proveer herramientas valiosas para diseñar procedimientos fuertes de seguridad.

Es de mucha importancia involucrar a todos los funcionarios que conforman la entidad en todos los procesos de la implementación del plan de Seguridad de la Información y que conozcan los beneficios del buen manejo y aplicación de ellos en sus labores.

Es de suma importancia que la entidad cuente con claras y precisas políticas de seguridad de información, como también que estén bien estructuradas, porque estas guiaran la conducta personal y profesional de todos los funcionarios de la secretaría, haciendo que la entidad trabaje bajo las mejores prácticas de seguridad y cumplimiento de los requisitos legales a los cuales está obligada.

Un programa de sensibilización sobre seguridad de la información da a conocer y a concientizar a los empleados de la secretaría sobre los riesgos a lo que se exponen los sistemas de información, generando en ellos buenas prácticas y compromisos respecto a las actividades que se deben tener sobre seguridad de la información.

Es de suma importancia que las entidades públicas tengan digitalizadas en su totalidad todos los expedientes de sus funcionarios, con esto les facilitará dar cumplimiento con mayor rapidez a los tramites que se tengan que realizar con estos activos, como también tener una copia digital de estos expedientes en un lugar seguro no se perdería la información si sufriere una destrucción total o parcial por parte de personal ajeno o propio de la entidad, o por desastres como inundaciones y fuego.

BIBLIOGRAFIA

[1] Modelo de Seguridad y Privacidad de la Información (MSPI). [En línea]. Available: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

[2] El portal de ISO 27001 en Español. [En línea]. Available: http://www.iso27000.es/iso27000.html

[3] ¿Qué es un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001?. [En línea]. Available: https://www.isotools.org/2016/07/07/sistema-gestion-seguridad-la-informacion-basado-la-norma-iso-27001/

[4] SGSI - Blog especializado en Sistemas de Gestión de Seguridad de la Información. [En línea]. Available: http://www.pmg-ssi.com/2015/07/que-es-sgsi/

[5] Universidad Pedagógica Experimental Libertador, Manual de Tesis de Grado y Especialización y Maestría y Tesis Doctorales, 2002. [En línea]. Available: http://neutron.ing.ucv.ve/NormasUPEL2006.pdf

[6] Alejandría Repositorio Comunidad. [En línea]. Available: http://alejandria.poligran.edu.co/

[7] Decreto Número 1078 del 26 de Mayo de 2015. [En línea]. Available: http://www.mintic.gov.co/portal/604/articles-9528_documento.pdf

ANEXOS

Pág.

ANEXO 1
POLÍTICA Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas de seguridad de la información se han dividido en cinco partes, las cuales son:

- La política general de seguridad de la información
- Alcance y aplicabilidad.
- Nivel de cumplimiento.
- Las políticas específicas.
- Los objetivos de la seguridad de la información.

La política general de seguridad de la información

Es la declaración global que realiza la directiva de la secretaría de educación con respecto a la protección de los activos que son manipulados por funcionarios y personal externo a la entidad, adicionalmente los activos como lo son hardware y software que son esenciales para el manejo en los procesos de talento humano, dando con esto un apoyo a la ejecución del sistema de gestión de seguridad de la información la cual se llevará a cabo por medio la creación de procedimientos, documentos y políticas, donde se documentarán las responsabilidades globales y específicas de cada recurso humano que intervengan el objetivo misional del área talento humano.

La secretaría de educación departamental y el área de talento humano busca establecer políticas de acuerdo con los objetivos de seguridad para:

1. Disminuir aquellos riesgos que afectan los objetivos misionales de la secretaría.
2. Proteger a cabalidad la información.
3. Acatar los principios misionales de la secretaría.
4. Buscar que la comunidad educativa no pierda la confianza en la secretaría.
5. Concientizar al desarrollo de la innovación tecnológica en la secretaría de educación.
6. Salvaguardar los activos de información de la secretaría.
7. Implementar políticas enfocadas a la seguridad de los activos de la secretaría.
8. Realizar procedimientos que estén siempre enfocados en la protección de la información.
9. Diseñar y colocar en práctica el SGSI.

10. Fortalecer en los funcionarios de la secretaría y personal externo conocimiento sobre seguridad de la información.
11. Frente a incidentes mantener en funcionamiento y continuidad los procesos de la secretaría.

Alcance y aplicación.

Esta política es aplicada a todos los empleados, contratistas y proveedores del área de talento humano de la secretaría de educación y personal que visita la secretaría de educación.

Nivel de Cumplimiento.

Todo el personal enmarcado en el alcance y aplicación deberá dar cumplimiento total de la política.

A continuación se establecerán políticas que soportan el SGSI del área de talento humando de la secretaria de educación.

1. El área de talento humano de la secretaría de educación, ayuda a desarrollar, implementar, operar y mejorar de forma periódica el SGSI, manejando estándares claros y alineados a los procesos.
2. El área de talento humano de la secretaría de educación, mantendrá la disponibilidad de la información creada, procesada, transmitida o resguardada en su proceso misional, evitando impactos operativos, legales o financieros con el incorrecto uso de esta, para evitar eso se aplicaran controles de acuerdo a la clasificación de la información.
3. El área de talento humano de la secretaría de educación, mantendrá la integridad de la información de aquellas amenazas originada por los funcionarios o agentes externos al área.
4. El área de talento humano de la secretaría de educación, protegerá la infraestructura que soporta su proceso misional.
5. El área de talento humano de la secretaría de educación, controlara el acceso a la información, a los sistemas y recursos de red que estén en su entorno.
6. El área de talento humano de la secretaría de educación, avalará la disponibilidad de sus procesos y continuidad de la operación si sucediera algún incidente.
7. El área de talento humano de la secretaría de educación, mantendrá el cumplimiento de aquellas obligaciones regidas por la ley.
8. Los empleados administrativos como la directiva de la secretaría son responsable en la protección de la información.

El incumplimiento a estas políticas por parte de funcionarios y personal externo podrá incurrir delito administrativo o penal según la normatividad de la secretaría y leyes o decretos establecidas por el gobierno nacional y territorial.

Las políticas específicas

1. Política para dispositivos móviles

La secretaría de educación dará a conocer a los empleados aquellas condiciones para el manejo adecuado de los dispositivos móviles de uso institucional o personal que ayude a cumplir los objetivos misionales, adicionalmente se encargará de velar por el buen uso de los dispositivos y servicios suministrados.

Se estipularan unas normas que van dirigidas a los funcionarios del área de talento humano de la secretaría:

- Los empleados no deben usar los dispositivos de la secretaría en sitio no seguros y que no brinden confianza de seguridad física para evitar incidentes
- Los funcionarios no deben instalar softwares, si necesitan instalar un programa para cumplimiento de sus funciones deberán solicitar un requerimiento al área de sistemas para su respectiva evaluación e instalación.
- Los funcionarios deben permitir la instalación de actualizaciones cada vez que el dispositivo se los pida, y estará controlado por el área de sistemas de la secretaría de educación
- No está permitido a los funcionarios el resguardo de información personal en los dispositivos asignados por la secretaría de educación.
- Está restringido al personal la modificación de las configuraciones de los equipos las cuales son realizadas por el área de sistemas de la secretaría de educación
- Los funcionarios no deben de sacar de la secretaría de educación los dispositivos sin autorización del área de sistemas.

2. Política de medios de almacenamientos extraíbles

El uso de medios de almacenamiento extraíbles en la red de la secretaria de educación estará controlado por el área de sistemas, con el fin de proteger la información.

Se estipularan unas normas que van dirigidas a los funcionarios del área de talento humano de la secretaría

- Los funcionarios de talento humano y personal externo no debe utilizar otros sistemas de almacenamiento que no sean los que se provea por el área de sistemas de la secretaría.

- Los funcionarios de talento humano son responsable del cuidado de los dispositivos de almacenamiento que se les ha asignado por parte del área de sistemas de la secretaría de educación.
- Los funcionarios de talento humano no deben realizar ninguna modificación a la configuración que el área de sistemas realice a los medios de almacenamientos.
- Los funcionarios no deben de sacar de la secretaría de educación los dispositivos extraíbles de almacenamiento sin autorización del área de sistemas.
- Antes de utilizar un medio de almacenamiento extraíble, el funcionario debe escanear este medio por el antivirus de su equipo de trabajo.

3. Política de responsabilidades de acceso de los funcionarios

Los funcionarios del área de sistemas de la secretaria de educación son los encargados de realizar el compromiso con los empleados, para el uso correcto y responsable de los recursos informáticos que quedan en su poder, como también la información que tengan permitida.

Se estipularan unas normas que van dirigidas a los funcionarios del área de talento humano de la secretaría:

- Los datos de autenticación a los sistemas dados a los funcionarios no pueden ser compartidos con otras personas.
- Los funcionarios con acceso a los servicios de red y sistemas deben cambiar periódicamente las contraseñas.
- Todos los funcionarios autorizados se hacen responsables de las acciones ejecutadas en los servicios de red y sistemas que posee la secretaría.
- Cuando una persona deja de laborar, el líder de talento humano debe enviar el un documento de baja del usuario al área de sistemas.

4. Política de control de accesos

El área de sistemas de la secretaría de educación es la encargada de que las redes estén protegidas por medio de controles físicos o lógicos, limitando el acceso a las personas no autorizadas.

Se estipularan unas normas que van dirigidas a los funcionarios del área de talento humano de la secretaría:

- Los nuevos funcionarios de talento humano antes de acceder a la red deben ser autorizados por el jefe de talento humano, el cual envía al área de sistemas el documento de creación de cuentas nuevas y el documento de confidencialidad debidamente firmado.

- Los funcionarios que deseen conectar sus dispositivos personales a la red de la secretaría deben cumplir ciertos requisitos de conexión y estar autorizado por el área de sistemas.
- Cada persona de talento humano debe proteger sus usuarios y contraseñas, no concederlos a otras personas, estas son únicas e intransferibles.

5. Política de protección contra el software malicioso

La secretaría de educación proporciona las herramientas necesarias para proteger la información y recursos tecnológicos para que no sean afectados por software malicioso.

El área de talento humano se encargará de hacer cumplir el plan de concienciación de seguridad en los funcionarios.

Se estipularan unas normas que van dirigidas a los funcionarios del área de talento humano de la secretaría:

- Los funcionarios de talento humano no deben deshabilitar o borrar el software de protección que se encuentra instalado en los equipos de trabajo.
- Los funcionarios de talento humano cuando vayan a utilizar los medios externos de almacenamiento deben revisarlos con el antivirus.
- Los funcionarios cuando bajen archivos del correo deben revisarlos con el antivirus.
- Si el funcionario detecta o sospecha de infección por software malicioso en su equipo de trabajo debe pasar una notificación inmediatamente al área de sistema para que el equipo sea intervenido.
- Los documentos que bajen de la red deben ser de fuentes conocidas y seguras, seguidamente revisados por el antivirus.

6. Política de respaldo de la información

La secretaría de educación garantiza los mecanismos para que el área de sistema lleve a cabo el proceso de generación de las copias de seguridad de todos los sistemas de información y de cada estación de trabajo.

También la secretaría de educación contará con una bóveda fuera de las instalaciones para que se guarden estas copias de seguridad.

Se estipularan unas normas que van dirigidas a los funcionarios del área de talento humano de la secretaría:

- Los funcionarios de talento humano tendrán que guardar todos los días la información importante que deseen para copia de seguridad en una carpeta especial en su equipo de trabajo creada por el área de sistemas.
- El funcionario no deberá borrar la carpeta para las copias de seguridad que es creada por el área de sistemas en su estación de trabajo.
- No podrá guardar información personal en esta carpeta, solo información para su ejecución de sus funciones de su puesto de trabajo.
- Si necesitan restablecer alguna información pedirán un requerimiento de restablecimiento de copia de seguridad al área de sistemas.

7. Política de escritorio limpio y pantalla limpia

La secretaría de educación y su área de talento humano definen las normas para disminuir el riesgo del acceso no permitido a los sistemas de información y estaciones de trabajo a cualquier hora.

Se estipularan unas normas que van dirigidas a los funcionarios del área de talento humano de la secretaría:

- Todos los funcionarios de la secretaría de educación cuando no estén laborando en los puestos de trabajo deben mantener el escritorio sin información que comprometan la seguridad de ésta misma.
- Todos los funcionarios de la secretaría de educación cuando no estén laborando en los equipos de trabajo deben mantener bloqueada la pantalla de sus computadores y deben colocarle clave de autorización de entrada.
- Cuando se deba imprimir documentos privados de la secretaría de educación el funcionario tiene que archivarlos al instante en un lugar seguro.

8. Política de transferencia de información

La secretaria de educación certificará la integridad y disponibilidad de la información cuando se necesite que sea copiada o transferida con otras áreas internas o entidades externas, e igual se establecerán los respectivos procedimientos y controles que sean necesarios para esta actividad.

Se estipularan unas normas que van dirigidas a los funcionarios del área de talento humano de la secretaría:

- Los funcionarios no deben compartir vía electrónica información que sea muy importante para la secretaría.
- Está restringido el intercambio telefónicamente de información importante de la secretaría.
- Los funcionarios de talento humano deben proteger la información que utilizan para su labor cotidiana y no divulgarla por medios no autorizados.

- Los funcionarios de talento humano deben dejar constancia en el sistema de atención al ciudadano de la información que den por respuesta a requerimientos de ciudadanos o entidades de control.

9. Política de Uso de Correo Corporativo

La secretaria de educación siendo consiente del uso del correo electrónico para comunicación de los funcionarios de la secretaría y otras entidades, facilitará que la utilización sea segura, manteniendo el respeto a los principios misionales de protección de la información por parte de todos los funcionarios.

Se estipularan unas normas que van dirigidas a los funcionarios del área de talento humano de la secretaría:

- La información que se envíe por correo corporativo debe ser únicamente información de carácter institucional.
- No debe enviar por el correo corporativo información personal.
- La información que se encuentra en estos correos corporativos son propiedad de la secretaría de educación
- Las cuentas asignadas a los funcionarios son únicamente de cada funcionario y no pueden utilizar otras cuentas que no sean de su autorización.
- Está prohibido el envío de información de cadenas y toda clase de información que no pertenezca al funcionamiento de los procesos de la secretaría de educación.
- Los mensajes enviados deben conservar las características e imagen corporativa establecidas por la secretaría de educación.
- Está prohibido enviar y abrir archivos ejecutables por el correo corporativo, si le llega uno a su correo borrar inmediatamente o informar al área de sistema para que sea examinado.
- Está prohibido abrir los correos personales en las instalaciones de la secretaría.

10. Política uso del uso de Internet

Todos los sistemas de información de la secretaría de educación requieren de conexión a internet, por lo tanto se garantizará por parte de la secretaría la disponibilidad del internet a los empleados para que cumplan con el desarrollo de sus funciones.

El área de sistemas con la directiva de la secretaría buscarán un mecanismo de registrar todas las páginas que sean visitadas por los funcionarios.

Se estipularan unas normas que van dirigidas a los funcionarios del área de talento humano de la secretaría:

- Los funcionarios de talento humano que utilizan el servicio de internet, no deben descargar material desconocido, ni visitar sitios de internet no seguros.

- Los funcionarios de talento humano deben utilizar el internet únicamente para dar cumplimiento a sus funciones laborales.
- Las páginas web que no son para el desarrollo de los procesos de la secretaría serán bloqueadas por parte del área de sistemas.
- Se les prohíbe a los funcionarios navegar por páginas web que no estén relacionadas con el trabajo de la secretaría y que por cualquier motivo no hayan sido bloqueadas por el área de sistemas.

11. Política de capacitación y sensibilización

La secretaría de educación consciente de la importancia en la formación de todo el personal administrativo en temas de protección de la información, la alta dirección proporcionará los recursos para implementar un plan de trabajo de concienciación de protección de la información.

Se estipularan unas normas que van dirigidas a los funcionarios del área de talento humano de la secretaría:

- El líder de talento humano tiene que estar comprometido en la ejecución del plan de concienciación de protección de la información.
- Los capacitados en seguridad de la información son cada uno de los funcionarios públicos que laboran y entran por primera vez a la secretaría.
- Es de obligatoriedad que todos los funcionarios públicos, tanto los antiguos como los nuevos que entran a la secretaría realicen las actividades propuestas en el plan de concienciación sobre seguridad de la información.
- El encargado de talento humano debe realizar y revisar periódicamente los indicadores que demuestran el desarrollo del plan de concienciación sobre seguridad de la información.
- En el área de talento humano se debe hacer firmar el compromiso y obligaciones por parte de los funcionarios cuando sean capacitados.

Los objetivos de la seguridad de la información

- Impulsar en todo el personal administrativo de la secretaría de educación el aseguramiento que se debe tener con el manejo de información.

- Realizar las debidas acciones preventivas y correctivas después de ejecutar el programa de riesgos de información.

- Oficiar los riesgos en seguridad de información para conocer su criticidad y poder ser asumidos o minimizados por medio de controles.

- Proteger la información y la tecnología utilizada para el procesamiento de ésta, en cumplimiento de las funciones de los empleados administrativos, asegurando los principios de protección de la información.

- Estar en la vanguardia de las nuevas técnicas, procedimientos y normas de seguridad sobre información que haya lugar a nivel nacional y mundial.

- Realizar periódicamente control interno sobre el SGSI para su correcto funcionamiento.

ANEXO 2
METODOLOGIA DE RIESGOS DE SEGURIDAD DE LA INFORMACION Y SU DESARROLLO

Se personalizará una metodología sobre el análisis de riesgos de la información para la Secretaría de Educación con los activos del área de talento humano, y se estructura la metodología.

Para ello se tomará de guía la siguiente documentación:

- el modelo de seguridad y privacidad de la información (MSPI) de la estrategia de gobierno en línea (GEL), el cual está alineado a la norma internacional ISO 27001:2013, en las guías 5 y 7

En los siguientes puntos se evidenciarán los pasos a seguir para un análisis de riesgos sobre los activos de la información en la Secretaría de Educación:

- Gestión y clasificación de los activos de información
- Identificación y valoración de las amenazas
- Análisis del riesgo

En este proceso se llevaran a cabo dos puntos:

1. El diseño de la metodología de riesgo, los pasos a seguir para encontrar las vulnerabilidades de riesgos en los activos de información.
2. Ejecución de esta metodología con respecto a los activos de información del área talento humano para encontrar sus vulnerabilidades de riesgos.

1. DISEÑO DE LA METODOLOGÍA DE RIESGO

A. GESTIÓN Y CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Este capítulo permite a la secretaría clasificar los activos de información más importantes y que se tienen que proteger para cualquier ataque interno o externo, por lo cual se identifica todas sus características y el rol al interior que tienen en un proceso.

Se recomienda al que realiza la gestión de clasificación de activos preguntarse:

• ¿Qué activos son esenciales para que usted consiga sus objetivos?

• ¿Hay más activos que tenga que proteger por obligación legal?
• ¿Hay activos relacionados con los anteriores?

Las actividades que se deben tener en cuenta para realizar un inventario de activos son:

1. Definición
2. Revisión
3. Actualización y
4. Publicación.

Imagen 1. Procedimiento Para Inventario de Activos.[25]

Para la propuesta de este proyecto se basará en la etapa de Definición de los activos de información

1.1 Etapa Definición. Esta etapa tiene como objetivo determinar qué activos de información cuenta la secretaría en su proceso de talento humano. Para el caso del proyecto se identificarán 4 activos de información de un proceso misional.

La información básica o características del activo para su definición sería la siguiente:

A. Proceso: Nombre del proceso al que pertenece el activo.[26]
B. Nombre Activo: Nombre de identificación del activo dentro del proceso al que pertenece.[27]

[25] Guía para la gestión y clasificación de activos de información en https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdF.. Pág. 11
[26] Ibíd. página 12.

C. Descripción/Observaciones: Es un espacio para describir el activo de manera que sea claramente identificable por todos los miembros del proceso.[28]

D. Tipo: Define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores, en este caso del proyecto solo se trabajarán con los activos de información que corresponden a tipo datos e información que están almacenados en equipos magnéticos o en estado físico, entre ellos podemos tener: las bases de datos, los contratos, la documentación de un sistema, investigaciones hechas por la empresa, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros muchos más.[29]

E. Contenedor: Es el repositorio físico o lógico donde se guardan los activos de información.

F. Responsable: Es el personal de la secretaría encargado de los activos de información.

G. Clasificación: Hace referencia a la protección de información de acuerdo a Confidencialidad, Integridad y Disponibilidad, sobre los impactos legal, de imagen y operacional.[30]

Clasificación de acuerdo con la Confidencialidad	
INFORMACION PUBLICA RESERVADA (ALTA)	Los activos de Información en el proceso seleccionado son disponibles sólo para un proceso de la entidad y que en caso que se conozcan anticipadamente pueden conllevar un impacto negativo Alto de: • Impacto Legal: La entidad podría ser intervenida y sancionada por los entes de control. • Impacto Imagen: La credibilidad ante las organizaciones y entidades que utilizan las estadísticas. • Impacto Operacional: Los siguientes procesos de la entidad se detendrían automáticamente.
IINFORMACION PUBCLCA CLASIFICADA	Los activos de información en el proceso seleccionado son disponibles para todos los procesos de la entidad y que en caso de ser

[27] Ibíd. página 12.
[28] Ibíd. página 12
[29] Ibíd. página 12
[30] Ibíd. página 13

(MEDIA)	conocida por terceros sin autorización puede conllevar un impacto negativo medio de: • Impacto Legal: La entidad podría ser multada económicamente y demandada por terceros. • Impacto Imagen: La credibilidad por personas que investigan a diario las estadísticas emitidas por la entidad. • Impacto Operacional: Algunos procesos de la entidad se detendrían automáticamente.
INFORMACION PÚBLICA (BAJA)	Los activos de información en el proceso seleccionado puede ser entregados o publicados sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad de la Secretaría de Educación, y traiga con ello un impacto • Legal: No tendría ningún tipo de sanción económica o intervenida por las actividades de control del estado. • Imagen: No afectaría su imagen con respecto a terceros que utilizan las estadísticas de la entidad. • Operacional: No pararía las actividades en los procesos.
Clasificación de acuerdo con la Integridad	
1 (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo alto: • Impacto Legal: La entidad podría ser intervenida y sancionada por los entes de control. • Imagen: La credibilidad ante las organizaciones y entidades que utilizan las estadísticas. • Operacional: La no ejecución de los siguientes procesos de la Secretaría de Educación.

2 (MEDIA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo medio: • Legal: La entidad podría ser multada económicamente y demandada por terceros. • Imagen: La credibilidad por personas que investigan a diario las estadísticas emitidas por la entidad. • Operacional: Algunos procesos de la entidad se detendrían automáticamente.
3 (BAJA)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad en lo: • Legal: No tendría ningún tipo de sanción económica o intervenida por las actividades de control del estado. • Imagen: No afectaría su imagen con respecto a terceros que utilizan las estadísticas de la entidad. • Operacional: No pararía las actividades en los procesos.
Clasificación de acuerdo con la Disponibilidad	
1 (ALTA)	La no disponibilidad de los activos de información en el proceso seleccionado puede conllevar un impacto negativo alto en: • Legal: La entidad podría ser intervenida y sancionada por los entes de control. • Imagen: La credibilidad ante las organizaciones y entidades que utilizan las estadísticas. • Operacional: La ejecución de los siguientes procesos de la Secretaría de Educación.
2 (MEDIA)	Si hace falta una parte de los activos de información se podría continuar con los otros procesos de la entidad y tendría impacto en: • Legal: La entidad podría ser multada económicamente y demandada por terceros. • Imagen: La credibilidad por personas que investigan a diario las estadísticas emitidas por la entidad. • Operacional: Algunos procesos de la entidad se detendrían automáticamente.

3 (BAJA)	La no disponibilidad de los activos de información en el proceso seleccionado no causaran impacto negativo en: • Legal: No tendría ningún tipo de sanción económica o intervenida por las actividades de control del estado. • Imagen: No afectaría su imagen con respecto a terceros que utilizan las estadísticas de la entidad. • Operacional: No pararía las actividades en los procesos.

IMPACTO	CRITERIOS		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
LEGAL 1	• **ALTA**: si hay al menos una clasifiación Alta • **MEDIA**: Si no hay clasificación Alta y por lo menos una clasificación Media • **BAJA**: Si los tres impactos tienen clasifiación Baja	• **ALTA**: si hay al menos una clasifiación Alta • **MEDIA**: Si no hay clasificación Alta y por lo menos una clasificación Media • **BAJA**: Si los tres impactos tienen clasifiación Baja	• **ALTA**: si hay al menos una clasifiación Alta • **MEDIA**: Si no hay clasificación Alta y por lo menos una clasificación Media • **BAJA**: Si los tres impactos tienen clasifiación Baja
IMAGEN 2			
OPERACIONAL 3			

Clasificación del Activo	
ALTA (3)	Activos de información en los cuales la clasificación es ALTA si se cumple alguna de estas condiciones: 1. Dos de sus propiedad es calificada como Alta. 2. Tres de sus propiedades es calificada como Alta.

MEDIA (2)	Activos de información en los cuales la clasificación es MEDIA si se cumple alguna de las siguientes condiciones: 1. Una de sus propiedades es Alta y una media. 2. Una propiedad Alta y al menos una baja. 3. Todas las propiedades sean calificadas como Media
BAJA (1)	Activos de información en los cuales la clasificación es BAJA, cuando todos sus niveles de calificación es baja.

B. IDENTIFICACIÓN Y VALORACIÓN DE LAS AMENAZAS

En este punto se determinan las amenazas que afectarían a cada activo seleccionado en el punto anterior y se dará su valoración. Las amenazas son un conjunto de actividades que pueden causar daño a los activos de la secretaría.

Una amenaza puede causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad. Las amenazas pueden venir por parte de la naturaleza o por parte del ser humano y estas pueden ser originadas accidentalmente o deliberadamente, se recomienda identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo (ej. Acciones no autorizadas, daño físico, fallas técnicas) Algunas amenazas pueden afectar a más de un activo y en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.[31]

Una vez determinado que la amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, lo podemos determinar en:

Degradación: Cuán perjudicado resultaría el valor del activo

Dimensiones: De seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante, [D] Disponibilidad, [I] Integridad y [C] Confidencialidad.

Algunas amenazas que pueden afectar los activos de información pueden ser encontradas en la norma Magerit V3 en su Libro II - Catálogo de Elementos.[32]

[31] Guía de gestión de riesgos en http://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf, página 19

[32] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WaNcEum1vIU

Valoración de la Amenaza.

La valoración de las amenazas para la secretaría se llevará de acuerdo a las siguientes especificaciones, con el fin de determinar de una forma eficaz el valor o la degradación que dicha amenaza pueda afectar los activos de información.

Clasificación de acuerdo a la pérdida de Confidencialidad	
ALTA (3)	Se determina esta clasificación en el caso que la amenaza ocurra, la información será conocida por terceros sin autorización y puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
MEDIA (2)	Se determina esta clasificación en el caso que la amenaza ocurra la información es conocida por terceros sin autorización puede conllevar un impacto negativo medio para los procesos de la misma.
BAJA (1)	Se determina esta clasificación en el caso que la amenaza ocurra no afectaría confidencialidad de la información ya que esta puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.

Clasificación de acuerdo a la pérdida de Integridad	
ALTA (3)	Si la amenaza ocurre la Información podría perder exactitud y completitud lo cual puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
MEDIA (2)	Si la amenaza ocurre la Información podría sufrir pérdida de exactitud y completitud lo cual conllevaría un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado en la entidad.
BAJA (1)	Si ocurre la amenaza la pérdida de exactitud y completitud de la información no conlleva a un impacto significativo para la entidad o entes externos.

Clasificación de acuerdo a la perdida disponibilidad	
ALTA (3)	Al suceder la amenaza en el activo de información la no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
MEDIA (2)	Al suceder la amenaza en el activo de información la no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
BAJA (1)	Al suceder la amenaza en el activo de información la no disponibilidad de la información podría afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.

Criterios de Clasificación la Amenaza		
CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
ALTA (3)	**ALTA (3)**	**ALTA (3)**
MEDIA (2)	**MEDIA (2)**	**MEDIA (2)**
BAJA (1)	**BAJA (1)**	**BAJA (1)**

Confidencialidad	Integridad	Disponibilidad	Calificación
1	1	1	1
1	1	2	2
1	1	3	3
1	2	1	2
1	2	2	4
1	2	3	6
1	3	1	3
1	3	2	6
1	3	3	9
2	1	1	2
2	1	2	4
2	1	3	6
2	2	1	4
2	2	2	8
2	2	3	12
2	3	1	6

2	3	2	12
2	3	3	18
3	1	1	3
3	1	2	6
3	1	3	9
3	2	1	6
3	2	2	12
3	2	3	18
3	3	1	9
3	3	2	18
3	3	3	27

ALTA (100%)	La amenaza es ALTA en los Activos de información si se cumple alguna de estas condiciones: 1. Un criterio de nivel baja y dos de nivel alta. 1. Un criterio de nivel alta y dos criterios de nivel media. 2. Dos criterios de nivel alta y uno media. 3. Los tres criterios son de nivel alta
MEDIA (050%)	La amenaza es MEDIA en los Activos de información si se cumple alguna de estas condiciones: 1. Un criterio de nivel baja y dos de nivel media. 2. Un criterio de cada uno, baja, media y alta. 3. Dos criterios de nivel baja y dos alto
BAJA (010%)	La amenaza es BAJA en los Activos de información si se cumple alguna de estas condiciones: 1. Los tres criterios sean de nivel baja. 2. Dos criterios de nivel baja y una media. 3. Dos criterios de nivel baja y uno alto.

C. ANALISIS DEL RIESGO

Para este caso se priorizaron un par de aspectos para ser tenidos en cuenta al momento de analizar los riesgos identificados, como lo es Probabilidad e Impacto. En la primera se resume a la posibilidad de que suceda el riesgo, esta se puede medir por criterios de frecuencia, si se ha materializado se entiende por número de veces que ocurra el riesgo, o factibilidad en la cual se identifican la presencia de factores externos como internos que pueden dar ocurrencia al riesgo. Por la parte de Impacto entendemos las consecuencias que ocasionan a la entidad la materialización del riesgo.

Clasificación del Riesgo: Se da a partir de la probabilidad de la ocurrencia y el impacto que pueda causar. La probabilidad por el número de repeticiones que el riesgo se ha presentado en determinado tiempo o pueda presentarse, y el impacto se refiere a la magnitud de los efectos producidos.

En las siguientes tablas se verán los factores probabilidad y el impacto con sus niveles de calificación.

Tabla de Probabilidad: En la siguiente tabla se identificaran los valores de ocurrencia del riesgo sobre los activos de la información.

Análisis de los Riesgos Administrativos			
Probabilidad de que ocurra el riesgo			
Nivel	**Calificación**	**Descripción**	**Frecuencia**
1	Raro	Puede ocurrir solo en circunstancia excepcionales	Puede ocurrir menos de 2 veces anualmente.
2	Improbable	Puede ocurrir en algún momento	Ocurrencia 3 y 4 Veces anualmente
3	Posible	Podría ocurrir en algún momento	Ocurrencia entre 5 y 8 Veces anualmente
4	Probable	Probablemente ocurrirá en la mayoría de las circunstancias	Ocurrencia entre 8 y 12 veces anualmente
5	Casi Seguro	Se espera que ocurra en la mayoría de las circunstancias	Ocurrencia más de 12 veces anualmente

Tabla de Impacto: En las siguientes tablas se identificaran los valores con que se determinará el impacto que tiene la amenaza sobre los activos de la información.

Se calcula multiplicando la calificación de la amenaza que se identifica de 10% a 100% por la clasificación de los activos según sus características confidencialidad, integridad y disponibilidad en los niveles alto, medio y bajo.

Calificación de la Amenaza	**Clasificación del Activo**		
	ALTA (3)	**MEDIA (2)**	**BAJA (1)**
ALTA (100%)	3	2	1
MEDIA (050%)	1,5	1	0,5
BAJA (010%)	0,3	0,2	0,1

Estos valores se relacionan en la siguiente tabla: insignificante, menor, moderado, mayor y catastrófico según el resultado, y por lo grande de la empresa en tecnología, personal y la cantidad de millones que maneja la entidad

Nivel	Calificación	Descripción	Calificación Amenaza x Clasificación del Activo
1	INSIGNIFICANTE (1)	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad, el impacto este entre los rangos 0 y 100 millones.	0,1
2	MENOR (2)	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad, el impacto este entre los rangos 100 millones y 200 millones.	0,2
3	MODERADO (3)	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad, el impacto este entre los rangos 200 millones y 300 millones.	0,3 a 0,5
4	MAYOR (4)	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad, el impacto este entre los rangos de 300 millones y 400 millones.	1 a 1,5
5	CATASTRÓFICO (5)	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad, el impacto sea mayor de 400 millones.	2 a 3

Matriz de Calificación, Evaluación y respuesta a los riesgos.

MATRIZ DE CALIFICACION Y EVALUACION DE RIESGOS					
PROBABILIDAD	IMPACTO				
	INSIGNIFICANTE 1	MENOR 2	MODERADO 3	MAYOR 4	CATASTROFICO 5
Raro 1	*1B*	*2B*	*3M*	*4A*	*5A*
Improbable 2	*2B*	*4B*	*6M*	*8A*	*10E*
Posible 3	*3B*	*6M*	*9A*	*12E*	*15E*
Probable 4	*4M*	*8A*	*12A*	*16E*	*20E*
Casi seguro 5	*5A*	*10A*	*15E*	*20E*	*25E*

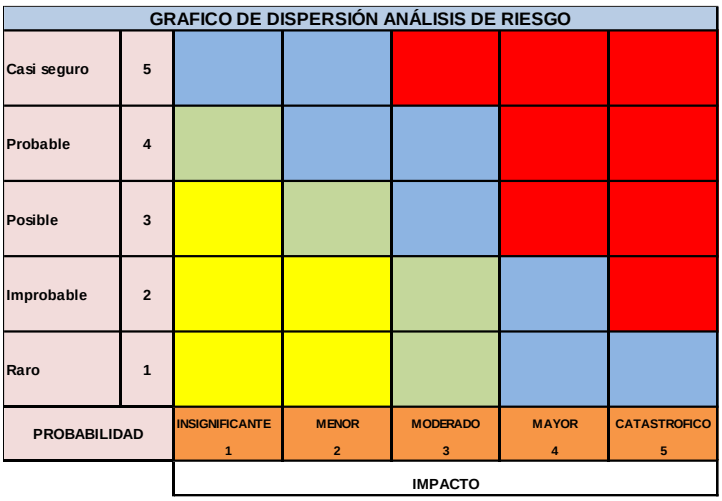
ZONA DE RIESGO O NIVEL DE EXPOSICION		
Zona	**Leyenda**	**Descripción**
BAJA	**B**	Riesgo BAJO, se puede asumir el riesgo
MODERADO	**M**	Riesgo MODERADO, se debe asumir o reducir el riesgo.
ALTA	**A**	Riesgo ALTO, debe ser reducido, evitado, compartido o transferido
EXTREMA	**E**	Riesgo EXTREMO, debe ser reducido, evitado, compartido o transferido

ZONA DE RIESGO	
1B	BAJO
2B	BAJO
3B	BAJO
4B	BAJO
3M	MODERADO
4M	MODERADO
6M	MODERADO
4A	ALTO
5A	ALTO
8A	ALTO
9A	ALTO
10A	ALTO
12A	ALTO
10E	EXTREMO
12E	EXTREMO
15E	EXTREMO
16E	EXTREMO
20E	EXTREMO
25E	EXTREMO

La información se mostrará cómo sigue en la siguiente figura.

Gráfico de dispersión ó de calor

En este gráfico se identificará de una manera más fácil la zona de calor donde se encuentran los riesgos detectados.



Opciones de tratamientos

- Evitar el riesgo
- Reducir el riesgo
- Compartir o Transferir el riesgo
- Asumir o Aceptar un riesgo

Acciones de mitigaciones o controles: Son los procedimientos efectuados para lograr asegurar el cumplimiento de los objetivos de la entidad Secretaría de Educación, los cuales tienen un efecto directo que mitigan los riesgos existentes.
Se pueden agrupar en controles internos, de seguridad y gestión de calidad, y sus objetivos serán:

Controles Internos: Buscar asegurar eficiencia y eficacia de las operaciones, cumplimiento de las leyes, normas y regulaciones y confiabilidad de la información.
Controles de Seguridad: Buscar asegurar la disponibilidad, confidencialidad e integridad de la información de la entidad.
Controles de Gestión de Calidad: Buscar asegurar la adecuada calidad, entrega y costo de las operaciones.

Los controles pueden tener la siguiente clasificación:

- Preventivos
- Protección
- Retención
- Transferencia

2. EJECUCIÓN DE LA METODOLOGÍA

En este punto se gestionará y se clasificaran los activos de información que se manejan en el área de talento humano de la secretaría de educación, luego se identificaran las amenazas que puedan causar daño a la información clasificada y por último los riesgos que pueden tener estas amenazas.

A. GESTIÓN Y CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Se basará en identificar cuatro activos de información, clasificación, contenedor, custodio e impacto que tenga el activo en la secretaría si se perdiera su confidencialidad, disponibilidad e integridad.

Proceso Apoyo: **TALENTO HUMANO**

Clasificación: Activos de Información

Contenedor: Servidor – Archivador

Custodio del activo: Jefe de Información **Responsable** Servidor de Nómina

		Disponibilidad			Integridad			Confidencialidad			Disponibilidad	Integridad	Confidencialidad	Clasificación
Nombre Activo	Descripción	Legal	Imagen	Operacional	Legal	Imagen	Operacional	Legal	Imagen	Operacional				
ASIN1. Registros completo de nómina	Documentación total del pago de todos los servidores públicos de la secretaría	BAJA (1)	MEDIA (2)	ALTA (3)	BAJA (1)	MEDIA (2)	ALTA (3)	ALTA (3)	MEDIA (2)	BAJA (1)	ALTA (3)	ALTA (3)	ALTA (3)	ALTA (3)

Por qué la clasificación?: Se considera alta por:

Disponibilidad Alta: La no disponibilidad del activo retrasaría los procesos misionales de la secretaría de educación, como el pago de nómina de todos los servidores que están a cargo de la secretaría

Integridad Alta: Cuya pérdida de exactitud y completitud conlleva a un impacto negativo como retrasar las funciones, no se llevaría como debe ser el proceso, ocasionando que no se le pueda pagar a los servidores públicos que está a cargo la secretaría

Confidencialidad Alta: Si se supiera de esta información podría tener alegatos jurídicos o demandas por parte de servidores porque ahí se manejan información privada.

Proceso Apoyo: **TALENTO HUMANO**

Clasificación: Activos de Información

Contenedor: Servidor - Archivador

Custodio del activo: Jefe de Información **Responsable** Operador de la información

		Disponibilidad			Integridad			Confidencialidad			Disponibilidad	Integridad	Confidencialidad	Clasificación
Nombre Activo	**Descripción**	**Legal**	**Imagen**	**Operacional**	**Legal**	**Imagen**	**Operacional**	**Legal**	**Imagen**	**Operacional**				
ASIN2. Información de servidores público	Se encuentra registrada la información de todos los servidores públicos que trabajan en la secretaría	BAJA (1)	MEDIA (2)	ALTA (3)	BAJA (1)	MEDIA (2)	ALTA (3)	ALTA (3)	BAJA (1)	BAJA (1)	ALTA (3)	ALTA (3)	ALTA (3)	ALTA (3)

Por qué la clasificación?: Se considera alta por:
Disponibilidad Alta: La no disponibilidad del activo retrasaría los procesos misionales de la secretaría de educación, y no se podría realizar otros procesos que necesitan esta información
Integridad Alta: Cuya pérdida de exactitud y completitud conlleva a un impacto negativo como retrasar las funciones, tendría consecuencias en realización de la nómina, etc.
Confidencialidad Alta: Si se supiera de esta información podría tener alegatos jurídicos o demandas por parte de servidores por que ahí se manejan información privada..

Proceso Apoyo: **TALENTO HUMANO**

Clasificación: Activos de Información

Contenedor: Archivo

Custodio del activo: Técnico Hojas de Vida **Responsable** Técnico Hojas de Vida

		Disponibilidad			Integridad			Confidencialidad			Disponibilidad	Integridad	Confidencialidad	Clasificación
Nombre Activo	Descripción	Legal	Imagen	Operacional	Legal	Imagen	Operacional	Legal	Imagen	Operacional				
ASIN3. Expedientes Hojas de Vida	Carpeta donde reposa la documentación completa desde que entró hasta el día que trabajó el servidor en la secretaría	BAJA (1)	MEDIA (2)	ALTA (3)	BAJA (1)	MEDIA (2)	ALTA (3)	ALTA (3)	MEDIA (2)	MEDIA (2)	ALTA (3)	ALTA (3)	ALTA (3)	ALTA (3)

Por qué la clasificación?: Se considera alta por:
Disponibilidad Alta: La no disponibilidad del activo retrasaría los procesos misionales de la secretaría de educación, y no se podría realizar otros procesos que necesitan esta información, cuando el servidor deba juvilarse necesita copia de toda esta información para enviar a la empresa de pensiones.
Integridad Alta: Si se pierde la integridad podría ocurrir en falsa información y esto afectaría en la juvilación de los servidores públicos, las estadísticas.
Confidencialidad Alta: Si se supiera de esta información podría tener alegatos jurídicos o demandas por parte de servidores por que ahí se manejan información privada..

Proceso Apoyo: **TALENTO HUMANO**

Clasificación: Activos de Información

Contenedor: Computador - Archivador

Custodio del activo: Técnico de recobros **Responsable** Técnico de recobros

		Disponibilidad			Integridad			Confidencialidad			Disponibilidad	Integridad	Confidencialidad	Clasificación
Nombre Activo	Descripción	Legal	Imagen	Operacional	Legal	Imagen	Operacional	Legal	Imagen	Operacional				
ASIN 4. Documentación de recobros	La documentación que se realiza a cada servidor público por incapacidades por enfermedades, para su cobro ante las entidades de seguridad social	ALTA (3)	MEDIA (2)	ALTA (3)	ALTA (3)	MEDIA (2)	ALTA (3)	BAJA (1)	MEDIA (2)	MEDIA (2)	ALTA (3)	ALTA (3)	MEDIA (2)	ALTA (3)

Por qué la clasificación?: Se considera alta por:

Disponibilidad Alta: La no disponibilidad del activo retrasaría los siguientes procesos misionales de la organización como ejemplo no poder recolectar la información estadística de un sector por demora en el diseño de formularios, la producción estadística, el análisis y difusión de la estadística, no se podría realizar estos cobros, tendríamos sanciones por parte de los entes de control

Integridad Alta: Cuya pérdida de exactitud y completitud conlleva a un impacto negativo como retrasar las funciones, no se sabría que cobrar a las entidades prestadoras de salud y se tendría sanciones legales por parte de los entes de control.

Confidencialidad media Esta información solo le compete a la secretaría, entes de control y entidades prestadoras de salud, pero no tendría inconvenientes que otras personas supieran de esta información.

Se observa en los resultados que los cuatro activos identificados en el área de Talento Humano de la Secretaría, son muy importantes para el desarrollo de todas las actividades de la secretaría y por lo tanto se puede realizar la identificación y valoración de las amenazas que puedan tener estos activos.

B. IDENTIFICACIÓN Y VALORACIÓN DE LAS AMENAZAS

Se determinaran los tipos de amenazas y dimensiones para los activos de información identificados en el área de talento humano:

Proceso Apoyo: TALENTO HUMANO **Clasificación:** Activos de Información **Contenedor:** Servidor – Archivador				**Custodio del activo:** Jefe de Información Técnica **Responsable:** Jefe de Información			
Nombre Activo	**Amenazas**	**Disponibilidad**	**Integridad**	**Confidencialidad**	**Calificación Amenaza**	**Clasificación Activo**	**Impacto**
ASIN1. Registros completo de nómina	1. Alteración y destrucción de datos en bases de datos	**ALTA (3)**	**ALTA (3)**	**BAJA (1)**	**ALTA (100%)**	**ALTA (3)**	**CATASTRÓFICO (5)**
ASIN1. Registros completo de nómina	2. Acceso por usuarios no autorizados a las base de datos	**ALTA (3)**	**ALTA (3)**	**ALTA (3)**	**ALTA (100%)**	**ALTA (3)**	**CATASTRÓFICO (5)**
ASIN1. Registros completo de nómina	3. Robo de información	**BAJA (1)**	**BAJA (1)**	**ALTA (3)**	**BAJA (010%)**	**ALTA (3)**	**MODERADO (3)**

Se puede observar que para el primer activo "Registros completo de nómina" las amenazas tienen un impacto catastrófico y moderado, el cual hay que realizar un análisis de riesgos.

Proceso Apoyo: TALENTO HUMANO							
Clasificación: Activos de Información		**Custodio del activo:** Jefe de Información					
Contenedor: Servidor - Archivador		**Responsable:** Operador de la Información					
Nombre Activo	**Amenazas**	**Disponibilidad**	**Integridad**	**Confidencialidad**	**Calificación Amenaza**	**Clasificación Activo**	**Impacto**
ADSO2. Información de servidores público	4. Acceso a datos sensibles o privados de los documentos del proceso	**BAJA (1)**	**MEDIA (2)**	**ALTA (3)**	**MEDIA (050%)**	**ALTA (3)**	**MAYOR (4)**
ADSO2. Información de servidores público	5. Modificación a información privada	**MEDIA (2)**	**ALTA (3)**	**ALTA (3)**	**ALTA (100%)**	**ALTA (3)**	**CATASTRÓFICO (5)**
ADSO2. Información de servidores público	6. Destrucción de copias de respaldos	**ALTA (3)**	**ALTA (3)**	**BAJA (1)**	**ALTA (100%)**	**ALTA (3)**	**CATASTRÓFICO (5)**

Se puede observar que para el segundo activo "Información de servidores públicos" las amenazas tienen un impacto catastrófico y mayor, el cual hay que realizar un análisis de riesgos.

Proceso Apoyo: TALENTO HUMANO							
Clasificación: Activos de Información		**Custodio del activo:** Ténico Hojas de Vida					
Contenedor: Archivo		**Responsable:** Ténico Hojas de Vida					
Nombre Activo	**Amenazas**	**Disponibilidad**	**Integridad**	**Confidencialidad**	**Calificación Amenaza**	**Clasificación Activo**	**Impacto**
ADSO3. Expedientes Hojas de Vida	7. Alteración y destrucción de la información por parte de entes externos	**ALTA (3)**	**ALTA (3)**	**BAJA (1)**	**ALTA (100%)**	**ALTA (3)**	**CATASTRÓFICO (5)**
ADSO3. Expedientes Hojas de Vida	8. Incendio por malas conexiones eléctricas.	**ALTA (3)**	**MEDIA (2)**	**BAJA (1)**	**MEDIA (050%)**	**ALTA (3)**	**MAYOR (4)**
ADSO3. Expedientes Hojas de Vida	9. Destrucción de información, Eliminar intencionalmente información, con el objeto de conseguir un beneficio o simplemente ocasionar perjuicio.	**ALTA (3)**	**ALTA (3)**	**BAJA (1)**	**ALTA (100%)**	**ALTA (3)**	**CATASTRÓFICO (5)**

Se puede observar que para el tercer activo "Expedientes Hojas de Vida" las amenazas tienen un impacto catastrófico y mayor, el cual hay que realizar un análisis de riesgos.

Proceso Apoyo: TALENTO HUMANO							
Clasificación: Activos de Información		**Custodio del activo:** Técnico de recobros					
Contenedor: Computador - Archivador		**Responsable:** Técnico de recobros					
Nombre Activo	**Amenazas**	**Disponibilidad**	**Integridad**	**Confidencialidad**	**Calificación Amenaza**	**Clasificación Activo**	**Impacto**
ADSO4. Documentación de recobros	10. Riesgo en la integridad del Software y la información, por la instalación de software sin autorización del área de sistemas o el coordinador de IT	**BAJA (1)**	**ALTA (3)**	**MEDIA (2)**	**MEDIA (050%)**	**ALTA (3)**	**MAYOR (4)**
ADSO4. Documentación de recobros	11. Perdida de información por error de Hardware	**ALTA (3)**	**BAJA (1)**	**BAJA (1)**	**BAJA (010%)**	**ALTA (3)**	**MODERADO (3)**
ADSO4. Documentación de recobros	12. Descarga y Propagación de virus por navegación en la web.	**ALTA (3)**	**ALTA (3)**	**ALTA (3)**	**ALTA (100%)**	**ALTA (3)**	**CATASTRÓFICO (5)**

Se puede observar que para el cuarto activo "Documentación de recobros" las amenazas tienen un impacto catastrófico, moderado y mayor, el cual hay que realizar un análisis de riesgos.

C. ANALISIS DEL RIESGO

Matriz del análisis de Riesgo. A continuación se mostrará la matriz de análisis de riesgo realizado a los activos y amenazas identificados en los puntos anteriores.

ANALISIS DE RIESGOS DE LA SECRETARIA DE EDUCACIÓN

PROCESO	IDENTIFICACIÓN DEL RIESGO					EVALUACIÓN				PLAN DE MANEJO	
	N°	ACTIVOS	AMENAZA	DESCRIPCIÓN	EFECTO	VALORACIÓN			ZONA DE VALORACIÓN DEL RIESGO	OPCION DE TRATAMIENTO	ACCIONES DE MITIGACIÓN O CONTROLES
						P	I	C			
TALENTO HUMANO	1	**ASIN1. Registros completo de nómina**	1. Alteración y destrucción de datos en bases de datos	Los usuarios con responsabilidades de instalación y operación pueden cometer errores en sus procesos	Pérdida de la información del registro completo del diseño de un sistema.	2	5	10E	EXTREMO	Reducir el riesgo	• Copias de seguridad.
	2	**ASIN1. Registros completo de nómina**	2. Acceso por usuarios no autorizados a las base de datos	Se tienen medidas de accesos como usuarios y claves no muy seguras por la cual facilita el acceso a las bases de datos por personal no autorizado.	Modificación de la información en bases de datos. Eliminación de datos en las bases de datos.	3	5	15E	EXTREMO	Reducir el riesgo	• Que las id usuario y contraseña no sean fácil de descifrar • Cambio periódica de contraseñas

PROCESO	IDENTIFICACIÓN DEL RIESGO					EVALUACIÓN				PLAN DE MANEJO	
	N°	ACTIVOS	AMENAZA	DESCRIPCIÓN	EFECTO	VALORACIÓN			ZONA DE VALORACIÓN DEL RIESGO	OPCION DE TRATAMIENTO	ACCIONES DE MITIGACIÓN O CONTROLES
						P	I	C			
TALENTO HUMANO	**3**	**ASIN1. Registros completo de nómina**	3. Robo de información	Pueden extraer información sensible por personal externo e interno de la empresa, causando desprestigio a la secretaría	Credibilidad de la secretaría. Suplantación en la información Disponibilidad de recursos.	1	3	3M	MODERADO	Reducir el riesgo	• Monitoreo de puertos. • Encriptar los datos de los discos duros en los pc's • Respaldo automáticamente la información • Colocar contraseña en la BIOS de los equipos. • Que todos los equipos tengan contraseña de arranque

PROCESO	IDENTIFICACIÓN DEL RIESGO					EVALUACIÓN				PLAN DE MANEJO	
	N°	ACTIVOS	AMENAZA	DESCRIPCIÓN	EFECTO	VALORACIÓN			ZONA DE VALORACIÓN DEL RIESGO	OPCION DE TRATAMIENTO	ACCIONES DE MITIGACIÓN O CONTROLES
						P	I	C			
TALENTO HUMANO	4	**ADSO2. Información de servidores público**	4. Acceso a datos sensibles o privados de los documentos del proceso	Acceder a la información de la documentación del proceso en las bases de datos y estaciones de trabajo.	Modificación de la documentación. Suplantación. Continuidad de los procesos.	2	4	8A	ALTO	Reducir el riesgo	• Encriptación de datos. • Implementación de contraseñas seguras.
	5	**ADSO2. Información de servidores público**	5. Modificación a información privada	Acceso a información por parte de personal interno y externo, otorgando así la modificación de los documentos aprobados para el diseño.	Modificación de los documentos aprobados. Demora en procesos. Disponibilidad de documentos.	2	5	10E	EXTREMO	Reducir el riesgo	• Asignar niveles de responsabilidad y acceso • Permisos de accesibilidad a la información por parte técnico interno. * Copias de seguridad
	6	**ADSO2. Información de servidores público**	6. Destrucción de copias de respaldos	Personal técnico no sigue procedimientos y por error eliminan datos clasificados al momento de realizar las copias de seguridad.	Perdida de Información Disponibilidad	1	5	5A	ALTO	Reducir el riesgo	• Realizar frecuentemente respaldos • Respaldos de información con claves de acceso • Tener copias de seguridad fuera de la secretaría. • Capacitación a funcionarios encargados del proceso de restauración copias

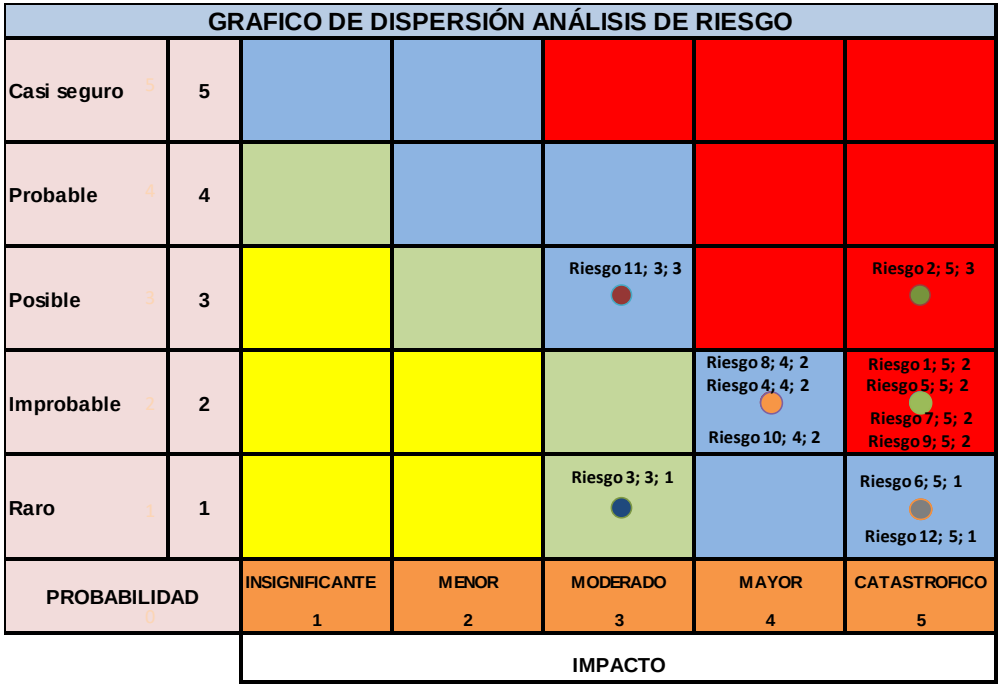
PROCESO	IDENTIFICACIÓN DEL RIESGO					EVALUACIÓN				PLAN DE MANEJO	
	N°	ACTIVOS	AMENAZA	DESCRIPCIÓN	EFECTO	VALORACIÓN			ZONA DE VALORACIÓN DEL RIESGO	OPCION DE TRATAMIENTO	ACCIONES DE MITIGACIÓN O CONTROLES
						P	I	C			
TALENTO HUMANO	7	**ADSO3. Expedientes Hojas de Vida**	7. Alteración y destrucción de la información por parte de entes externos	Personal técnico externo no conoce bien el proceso y puede eliminar la información de los diseños, extracción de documentos.	Socialización no autorizada de la información a otras empresas. Eliminación de los datos	2	5	10E	EXTREMO	Reducir el riesgo	• Copia de seguridad • Planificar las tareas del personal externo y realizar seguimiento. * Verificación de conocimiento del soporte técnico.
	8	**ADSO3. Expedientes Hojas de Vida**	8. Incendio por mala conexiones eléctricas.	Las malas conexiones eléctricas pueden causar incendios, por falta de un plan anual de verificación de redes y de cargas eléctricas.	Disponibilidad de la Información. Perdida de información. Disponibilidad de equipos Disponibilidad de personal.	2	4	8A	ALTO	Reducir el riesgo	• Copias de seguridad. • Adquirir equipos de protección para altos voltaje de corriente. • Revisión periódica de la red eléctrica.
	9	**ADSO3. Expedientes Hojas de Vida**	Destrucción de información, Eliminar intencionalmente información, con el objeto de conseguir un beneficio o simplemente ocasionar perjuicio.	Los usuarios con responsabilidad del manejo de la información, alteran, modifican o eliminan información no correspondiente a las labores indicadas	Disponibilidad de la Información. Modificación de la información Demora en los procesos Credibilidad de la secretaría.	2	5	10E	EXTREMO	Reducir el riesgo	• Tener un mecanismo que respalde automáticamente información en servidores • Brindar capacitaciones a los trabajadores en la importancia de seguridad de la información. • Verificación de permisos a los usuarios.

PROCESO	IDENTIFICACIÓN DEL RIESGO					EVALUACIÓN				PLAN DE MANEJO	
	N°	ACTIVOS	AMENAZA	DESCRIPCIÓN	EFECTO	VALORACIÓN			ZONA DE VALORACIÓN DEL RIESGO	OPCION DE TRATAMIENTO	ACCIONES DE MITIGACIÓN O CONTROLES
						P	I	C			
TALENTO HUMANO	**10**	**ADSO4. Documentación de recobros**	10. Riesgo en la integridad del Software y la información, por la instalación de software sin autorización del área de sistemas o el coordinador de IT	Se puede identificar software que no deberían estar instalados en los equipos, algunos de ellos sin licencia de funcionamiento (Crackeados) por programas que podrían ser dañinos en la seguridad de la información de la secretaría.	Disponibilidad de la información. Daño de equipos Extracción de información privada. Imagen de la empresa	2	4	8A	ALTO	Reducir el riesgo	• Manejo de instalación de software. • Privilegio de usuarios. • Seguridad acceso equipos externos.
	11	**ADSO4. Documentación de recobros**	11. Perdida de información por error de Hardware	El Hardware donde se encuentra la información presenta fallas de disco duro, puede afectar la disponibilidad de la misma y por ende el retraso en los procesos	Disponibilidad d ela información Perdida de la información. Imagen de la empresa	3	3	9A	ALTO	Reducir el riesgo	• Respaldar información automática en servidores • Antes de renovar un pc, revisarlo minuciosamente. • Realizar mantenimiento en los pc por lo mínimo dos veces al año • Plan Capacitación de servidores.

PROCESO	IDENTIFICACIÓN DEL RIESGO					EVALUACIÓN				PLAN DE MANEJO	
	N°	ACTIVOS	AMENAZA	DESCRIPCIÓN	EFECTO	VALORACIÓN			ZONA DE VALORACIÓN DEL RIESGO	OPCION DE TRATAMIENTO	ACCIONES DE MITIGACIÓN O CONTROLES
						P	I	C			
TALENTO HUMANO	**12**	**ADSO4. Documentación de recobros**	12. Descarga y Propagación de virus por navegación en la web.	Los usuarios ingresan a paginas no autorizadas o a plataformas externas las cuales pueden afectar la red y por ende los datos almacenados en los diferentes repositorios de la secretaría.	Disponibilidad de Información Perdida de información Imagen de la secretaría Daño de equipos Retrazos en los procesos	1	5	5A	ALTO	Reducir el riesgo	• Bloquear páginas no seguras en internet • Activación de Firewall • Chequear periódicamente el tráfico de red • Adquirir antivirus con licenciamiento empresarial • Actualización de antivirus. • Mantener activo los antivirus y con clave el panel de configuración.

CONVENCIONES PARA RIESGOS DE CORRUPCIÓN	PROBABILIDAD	P
	IMPACTO	I
	CALIFICACION	C

Gráfico de dispersión ó de colores. Gráfico de color donde ubica la calificación de los riesgos que tienen los activos identificados si ocurrieran las amenazas especificadas.



Observando el gráfico de dispersión y el análisis de riesgo, se puede calcular el porcentaje de estos riesgos en los niveles o zona de valoración:

- De los 12 riesgos 5 de ellos son de valoración Extremo, para un 41.6%
- 6 de ellos son de valoración Alta, para un 50%.
- 1 de valoración Moderado, para un 8.4%

Con esta especificación se puede saber el nivel de importancia de los riesgos y su posible impacto en la secretaría.

Opciones de tratamientos. La acción que se escogió para tratar todos los riesgos fue de reducirlos con controles, estos riesgo se podrán mitigar entre una probabilidad de 1 a 2 y un impacto de 1 a 2.

Acciones de mitigaciones o controles. Los controles propuestos se agruparon en la categoría de controles de seguridad, donde se busca asegurar la disponibilidad, confidencialidad e integridad de los activos de información seleccionados en la Secretaría de Educación del área de Talento Humano.

ACCIONES DE MITIGACIÓN O CONTROLES	APLICABILIDAD	CLASIFICACIÓN	VALOR DEL CONTROL	BENEFICIO
• Copias de seguridad.	Realizar la adquisición de Storage Empresariales. Servicio de custodia por entidad externa.	Protección	Realizar la compra de servidores storage empresariales para el manejo de la información para la replicación de los datos	Se mantendrá la integridad y disponibilidad del diseño del sistema con el fin de que sucede una eventualidad pueda ser restaurada en el menor tiempo posible y así mantener los procesos. La custodia de los discos duros preservará la integridad de los contenedores de activos y así estar disponibles en caso de una eventualidad catastrófica en las instalaciones de la secretaría.
• Id usuario y contraseña robustas. • Cambio periódica de contraseñas	Adquisición de Llaves de seguridad (smartCard) para el acceso remoto a los servidores de Bases de datos.	Prevención	Adquirir sistema de cifrado por medio de memorias llaves (USB), manteniendo limitado el acceso a las bases de datos.	Con la adquisición de las llaves tendremos el beneficio que las bases de datos vía acceso remoto desde los equipos de los administradores de los activos, en caso de mantenimiento y revisión, con el beneficio de proteger la integridad de los activos.
• Monitoreo de puertos.	Realizar procedimiento de lista de chequeo para el monitoreo en los diferentes dispositivos.	Prevención	No contiene valor el control debido que se estipulará en las funciones de los técnicos Internos.	Se mantendrá la seguridad de la secretaría esto con el fin de mitigar los ataques informáticos por parte de personal externo dando como resultado la disponibilidad del negocio y la integridad de los activos.

ACCIONES DE MITIGACIÓN O CONTROLES	APLICABILIDAD	CLASIFICACIÓN	VALOR DEL CONTROL	BENEFICIO
• Respaldar información automática en servidores	Configuración de tareas programadas de Backup en los servidores con una recurrencia semanal.	Protección	No se invertirá dinero por parte de la secretaría ya se utilizarán los recursos tecnológicos asignados.	Se tendrá disponibilidad semanal de la información lo cual trae como beneficio que los procesos no se detengan por parte de los activos estipulados de la información.
• Colocar contraseña en la BIOS de los equipos	Implementar seguridad en el sistema de arranque de los equipos	Protección	No se contará con costos en la implementación de este control por parte de la secretaría	Se tendrá más seguridad al momento de los desplazamientos que hace el personal a las diferentes sedes con los equipos portátiles, asegurando la integridad de los activos de la información en caso de pérdida o robo de las máquinas, obteniendo así control y no realizar compra de más equipos.
• Implementar contraseñas seguras de inicio de sesión en los equipos.	Fomentar procedimiento de activación de contraseñas al inicio de sesión	Prevención	No contará con valor económico este control debido que se utilizará con el personal técnico de la secretaría	Se obtendrá el beneficio que las personas que tienen acceso a los activos críticos tengan mejor seguridad y que ningún otro usuario o persona externa acceda a los mismos y poner en riesgo la integridad de los documentos.
• Realizar asignación de niveles de responsabilidad y acceso	Creación de procedimiento de otorgamiento en accesos a usuarios de acuerdo al nivel de responsabilidad en la secretaría	Protección	No se contempla la asignación de recursos para este control	Se tendrá más seguridad en el acceso a las bases de datos críticos y activos los cuales pueden ser utilizados por empleados descontentos para afectación de los procesos en la secretaría.
• Permisos de accesibilidad a la información por parte técnico interno	Verificación de recursos de acceso al personal interno. Seguimiento mensual a los accesos	Protección	No se asignará recursos económicos para las medidas de control.	Se evidenciará el nivel de acceso del personal interno para así estar seguros de los accesos que tienen el personal que solo los autorizados manejen la

ACCIONES DE MITIGACIÓN O CONTROLES	APLICABILIDAD	CLASIFICACIÓN	VALOR DEL CONTROL	BENEFICIO
				información y no correr el riesgo de que se eliminen por fallas en proceso o manipulación por parte del personal técnico.
• Tener copias de seguridad fuera de la secretaría.	Contemplar la opción de tercerización de copias de seguridad a entidad externa en custodia. (Empresa de seguridad Privada)	Protección	El valor de este control depende del mercado en las empresas	Con esta aplicabilidad se dispondrá de la integridad de los dispositivos de almacenamiento seguros, para cualquier eventualidad que suceda en las instalaciones, se cuente con los diseños de los activos intactos y poder implementar nuevamente los procesos si en dado caso se requiera.
• Capacitación a funcionarios encargados del proceso de restauración copias	Realizar procedimiento de restauración de datos Verificación de calificación del personal técnico.	Prevención	No se contará con asignación presupuestal para este control.	Integridad y disponibilidad manteniendo así la seguridad de los datos y no tener perjuicio en dado caso que se eliminen por error las bases de datos, dando como resultado el retraso de los procesos y la imagen de empleados a nivel interno.
• Planificar las tareas del personal externo y realizar seguimiento.	Lista de chequeo de los procesos a intervenir. Calificación del personal técnico externo. Referencia de la empresa contratada. Seguimiento al personal	Prevención	No se contará con recursos para el control debido que se hará con personal técnico interno de la secretaría	De acuerdo a los procedimientos aseguramos que el personal técnico externo pueda extraer información confidencial la cual afecte la continuidad del negocio como la imagen de la secretaría acarreando así perdidas de credibilidad en los datos de los activos que se manejan.
• Verificación de conocimiento del soporte técnico.	Pruebas de conocimiento técnicas. Cursos Online en plataformas gratuitas.	Prevención	No contiene valor el control debido que se estipulará en las funciones de los	Con esto obtenemos que el personal interno cumpla las tareas estipuladas dando como resultado la mejoro y eficiencia en los

ACCIONES DE MITIGACIÓN O CONTROLES	APLICABILIDAD	CLASIFICACIÓN	VALOR DEL CONTROL	BENEFICIO
			técnicos Internos.	procesos, manteniendo así la información al día para cuando se requiera necesaria suministrarla al estado.
• Adquirir equipos de protección para altos voltaje de corriente.	Compra de UPS	Protección	El valor depende como este en el mercado y la magnitud o grandeza de protección.	Se preservará el estado de los equipos, obteniendo una disponibilidad de los activos dando como beneficio que los procesos no se detengan por fallas en la infraestructura.
• Revisión periódica de la red eléctrica.	Mantenimiento de red eléctrica	Protección	El valor del control se estipula de acuerdo a los rubros que están estipulados en el plan de mantenimiento de la secretaría.	Se mantendrá la seguridad de que las conexiones eléctricas de los equipos no sufrirán ninguna alteración y posterior daño lo cual evitaría el remplazo de los mismos.
• Manejo de instalación de software.	Procedimiento de instalación de software	Prevención	No se contará con valor económico ya se realizará por personal técnico interno.	Se evidenciará las software maliciosos que puedan ser puente para la integridad, disponibilidad de información de la secretaría, equipos informáticos y así pueda afectar la imagen de la empresa y el retardo de los procesos.
• Seguridad acceso equipos externos.	Protección puertos de red y WIFI. Procedimiento de verificación equipos a ser conectados a la red inalámbrica.	Prevención	No se contará con valor económico para el manejo de este control por parte de la secretaría, solo disponibilidad del personal técnico Interno.	Se contará con mayor seguridad para evitar el acceso de virus o malware externo que contengan los equipos del personal externo, conllevando con la caída de los servicios y así afecte la disponibilidad de los procesos e imagen de la secretaría
• Respaldar información automática en servidores.	Creación de tareas de Backup	Prevención	No se contempla la asignación de recursos	Al contar con estos controles se dispondrá de disponibilidad, integridad y confiabilidad de los

ACCIONES DE MITIGACIÓN O CONTROLES	APLICABILIDAD	CLASIFICACIÓN	VALOR DEL CONTROL	BENEFICIO
	Selección de datos críticos		para este control	activos ya que en alguna eventualidad se recuperarán de forma rápida y así no afectaría los procesos e imagen de la secretaría.
• Realizar mantenimiento en los pc por lo mínimo dos veces al año	Mantenimiento de equipos con el personal técnico interno	Preventivo	El valor de este control se verá reflejado en el tiempo que demore el proceso de mantenimiento.	Se preservará la duración de los equipos para el correcto funcionamiento y así no adquirir adicionales por fallas de mantenimiento.
• Plan Capacitación de servidores.	Plan de disponibilidad de servidores mensualmente o anual	Preventivo	No se contempla la asignación de recursos para este control por parte de la secretaría	En esta implementación se tendrá a la mano la información de la disponibilidad de los servidores en temas de capacidad en dado caso que se requiera aumentar el nivel se sepa de una forma anticipada y así no tener contratiempos que afecten la disponibilidad de los procesos e imagen de la secretaría.
• Bloquear páginas no seguras en internet.	Plan de bloqueo páginas de internet. Procedimiento de acceso a WEB	Preventivo	No se invertirá dinero por parte de la secretaría y se utilizarán los recursos tecnológicos asignados.	Se mantendrán los activos informáticos libres de cualquier ataque por acceso a las páginas, adicionalmente se protegerá la suplantación de páginas conocidas y puedan afectar el funcionamiento de los procesos de la secretaría por vía de virus que puedan afectar la disponibilidad, integridad y disponibilidad de los activos de la información.
• Activación de Firewall			Se realizaran con	Se hará una ventana de mantenimiento para la

ACCIONES DE MITIGACIÓN O CONTROLES	APLICABILIDAD	CLASIFICACIÓN	VALOR DEL CONTROL	BENEFICIO
	Mantenimiento Mensualmente	Preventivo	personal técnico interno lo cual no requiere inversión de dinero.	actualización de los dispositivos los cuales se realizarían en fechas que sean no críticas para el desarrollo de los procesos, manteniendo así la publicación de los datos a todo el personal de la secretaría.
• Chequeo del tráfico de red	Lista de chequeo diaria del estado de la red.	Preventiva	No se invertirá dinero por parte de la secretaría.	Se tendrá disponibilidad para la verificación externa por parte del estado dando como resultado del beneficio de imagen de la secretaría.
• Adquirir antivirus con licenciamiento empresarial	Renovación de licencias de antivirus	Preventiva	El valor será lo que cueste en el mercado y la cantidad de adquisición	Con la adquisición de las licencias se mantendrán y preservarán los sistemas lógicos de los equipos y la seguridad que un virus pueda realizar modificación en los archivos de bases de datos manteniendo así la disponibilidad de los activos y la no demora en los procesos.
• Mantener antivirus actualizado en los equipos	Procedimiento de revisión definiciones actualizadas de antivirus	Preventiva	No se contará con valor económico asignado para esta actividad, ya que se realizará con personal técnico Interno.	Mantendrá la seguridad de los equipos ya que no se infectarán por archivos infecciosos que puedan dañar las máquinas y afecten el desarrollo de los procesos. Aumentando así el costo de los activos.

ANEXO 3
PLAN DE TRABAJO DE CONCIENCIACIÓN DE SEGURIDAD DE LA INFORMACIÓN

Objetivos del plan de concienciación

- Cumplir con las obligaciones que emana la legislación vigente, Ley 1581 de 2012, en la protección de los datos personales en Colombia.
- Garantizar que todos los servidores que laboran en la secretaría de educación puedan cumplir con su programa de entrenamiento sobre seguridad de información.
- Promover conciencia en protección de datos a los funcionarios de la secretaría de educación.
- Dar a conocer las obligaciones que tienen los empleados de la secretaría sobre la seguridad de la información.
- Concientizar a todos los trabajadores de la secretaría de cómo proteger la información.
- Concientizar a todos los trabajadores de la secretaría sobre los riesgos existentes que pueden causar pérdida y daño a la información.
- Lograr que todos los funcionarios de la secretaría se comprometan a tener cuidado de la información que manejan en sus actividades diarias.
- Cumplir con el 100% del programa de concienciación establecido para la seguridad de la información.

Destinatarios del plan de concienciación

Este plan de concienciación va dirigido al personal antiguo y nuevo que labora en el área de talento humano de la secretaría de educación.

Actividades a desarrollar en el plan de concienciación

1. ***Realizar el curso digital sobre seguridad de la información a los nuevos y antiguos***. Este curso se basa en conceptos y en buenas prácticas para el manejo de la seguridad de información, también contempla temas de legislación colombiana.

   Objetivo: Realizar por solo una vez el curso digital sobre seguridad de la información a funcionarios nuevos y antiguos que no hayan realizado el curso.

   Herramienta: El curso se realiza vía internet.

   Tiempo: Se realiza una sola vez y dura un semestre.

   Indicador: Cantidad de funcionarios que realizan el curso digital sobre seguridad de la información (CFRCDSI).

   CFRCDSI = (# de funcionarios que presentaron el curso virtual / # funcionarios del área de talento humano) *100%.

2. ***Comunicados periódicos sobre temas de seguridad de la información***. Cada comunicado contendrá temas sobre el buen manejo que se debe dar a la seguridad de la información.

   Objetivo: Realizar mensualmente las comunicaciones en temas de seguridad de información o buenas prácticas a los funcionarios de talento humano de la secretaría de educación

Se pueden hacer comunicados sobre los siguientes temas:

- ✓ Sobre cumplimiento de la política de seguridad de la secretaria de educación.
- ✓ Sobre las contraseñas, la manera correcta sobre el manejo en general de las claves que utilizan en los aplicativos y computadoras
- ✓ Antivirus, el deber que tienen todos los funcionarios en examinar con el antivirus todos los discos externos antes de utilizarlos.
- ✓ Sobre los correos electrónicos, el uso debe ser únicamente laboral, no enviar cadenas o datos personales.
- ✓ Sobre el manejo de Internet, se le puede dar a conocer a los funcionarios que está o que no está permitido sobre el internet.
- ✓ Sobre copias de seguridad de los datos: informar a todos los funcionarios el proceso de copias de seguridad que maneja la secretaría de educación y qué importancia tiene este con respecto a la seguridad de la información.
- ✓ Pasos a seguir después de un incidente, dar a conocer a los funcionarios de la secretaría los pasos a seguir en el caso que existiera un incidente.
- ✓ Sobre seguridad de los dispositivos de almacenamiento USB, explicar el tratamiento que se debe tener en el manejo de estos dispositivos.
- ✓ Sobre el envío de información, dar a conocer a los funcionarios las medidas de seguridad que se aplican en el envío de información importante de la secretaría.
- ✓ Sobre el software, dar a conocer a los funcionarios el riesgo que tiene el software no permitido y no controlado instalado en los equipos de cómputo para la seguridad de la información de la secretaría.
- ✓ Sobre la seguridad de los equipos, la importancia que tienen los protectores de pantalla o bloqueo de PC después de cierto tiempo de estar inactiva las pantallas para la seguridad de la información en la secretaría.[33]

[33] ISO 27001 – ¿Cómo confeccionar un plan de concienciación sobre la Seguridad de la Información? en http://www.pmg-ssi.com/2014/06/iso-27001-como-confeccionar-un-plan-de-concienciacion-sobre-la-seguridad-de-la-informacion/

- ✓ Buenas prácticas sobre escritorio y pantalla limpia, proporcionar a los funcionarios de la secretaría la importancia que tiene este tema para la protección de la información en la secretaría de educación.

Herramientas: Se pueden realizar en cartillas, volantes o videos con documentación gratuita que existe en la web.

Tiempo: Estos temas se preparan y se envía a los funcionarios uno por mes durante los 12 meses.

Indicador: Cantidad de comunicaciones de seguridad de la información (CCBPSI)

CCBPSI = (# Comunicados realizado al área de talento humano / # Comunicados programados durante el año) *100%.

3. ***Realizar concursos sobre seguridad de la información****:* Los concursos son buena actividad para que los funcionarios se interesen más por la seguridad de la información.

Objetivo: Realizar un concurso al año sobre seguridad de la información a los funcionarios de talento humano de la secretaría de educación.

Herramienta: Puede ser una sopa de letras, un crucigrama, etc.

Tiempo: Se realiza una sola vez al año.

Indicador: Cantidad de funcionarios que realizan el concurso sobre seguridad de la información (CFRCSI).

CFRCSI = (# de funcionarios que presentaron concurso virtual / # funcionarios del área de talento humano) *100%.

4. ***Realizar charlas de concienciación a los funcionarios***: Las charlas refrescan los temas de seguridad de la información a los funcionarios.

   Objetivo: Realizar charlas periódicas en el año sobre seguridad de la información a los funcionarios de talento humano de la secretaría de educación.

   Herramienta: Se realizan por medio de presentaciones de powerpoint y se realizan en el salón de junta de la secretaría.

   Tiempo: Se realiza 4 charlas al año.

   Indicador: Cantidad de charlas realizadas de seguridad de la información (CCRESI).

   CCRESI = (# de charlas realizadas al año / # de charlas programadas al año) *100%.

Cronograma de actividades

Programa	MESES												META (%)
	1	2	3	4	5	6	7	8	9	10	11	12	
Curso Digital				Número de Funcionarios									# Funcionarios 100%
Comunicados periódicos	1	1	1	1	1	1	1	1	1	1	1	1	12 100%
Concurso										1			1 100%
Charlas			1			1			1			1	4 100%

Seguimiento del Plan de Trabajo

Muestra el porcentaje de cumplimiento que se lleva en el transcurso del año, al finalizar el año se tiene que tener un cumplimiento del 100%.

Para saber el porcentaje de cumplimiento por actividad se calcula por medio del indicador de cada actividad, de la siguiente manera:

1. ***Realizar el curso digital sobre seguridad de la información a los nuevos y antiguos***

   CFRCDSI = (# de funcionarios que presentaron el curso virtual / # funcionarios del área de talento humano)*100%.

2. ***Comunicados periódicos sobre temas de seguridad de la información.***

   CCBPSI = (# Comunicados realizado al área de talento humano / # Comunicados programados durante el año) *100%.

3. ***Realizar concursos sobre seguridad de la información***

   CFRCSI = (# de funcionarios que presentaron concurso virtual / # funcionarios del área de talento humano) *100%.

4. ***Realizar charlas de concienciación a los funcionarios***

   CCRESI = (# de charlas realizadas al año / # de charlas programadas al año) *100%.

Para saber el total de cumplimiento del plan de trabajo se debe averiguar de la siguiente manera:

Meta Total Plan de Trabajo (MTPT) = (CFRCDSI + CCBPSI + CFRCSI + CCRESI) / 4

ANEXO 4
PLAN DE TRABAJO PARA LA DIGITALIZACIÓN DE TODOS LOS EXPEDIENTES

Para el respaldo de la información con respecto a la digitalización de las hojas de vida se debe tener encuesta:

- La secretaría de educación cuenta con unos 4.000 expedientes de hojas de vida entre servidores públicos activos e inactivos.
- Los equipos de cómputos y escáner pueden ser prestados por parte de las Instituciones Educativas que son vigiladas por la secretaría y así se ahorraría la compra de estos equipos.
- Revisión de estos equipos por parte del profesional universitario encargado del área de sistemas.
- Adecuación de la oficina con su parte eléctrica y red separada de la secretaría.
- El personal para el escaneo se realizará por medio de alumnos pasantes de una institución local con pensum en ofimática, entre ellas puede ser el SENA
- Compra de discos duros externos y capacitación al personal del subproceso historias laborales.

Para tener en cuenta la capacidad de almacenamiento de estas hojas de vida se realiza la siguiente formula:

Cantidad MB en una Hoja de vida = 100 MB en promedio.

Total de Hojas de vida = 4.000

Espacio total Necesitado = Cantidad MB en una Hoja de vida x Total de Hojas de vida

Espacio total Necesitado = 100 MB * 4.000 = 400.000 MB = 400 GB

Se pueden conseguir unos 3 discos duros de 1000 GB cada uno para tener copias de seguridad.

Para escanear las 4.000 hojas de vida en dos meses se tendría en cuenta la siguiente fórmula para hallar cantidades de equipos prestados y digitadores:

Tiempo revisión una hoja de vida = 20 minutos por promedio

Tiempo de escaneo una hoja de vida: 15 minutos por promedio

Total de tiempo por hoja de vida = 20+15 = 35 minutos

Total de equipos de cómputos para trabajar prestados = 10 equipos

Total de tiempo trabajado en 2 meses = 44 días hábiles de trabajo x 8 horas = 352 horas = 21.100 min

Total digitadores = Total de tiempo por hoja de vida * Total de Hojas de vida / Total de tiempo trabajado en 2 meses

Total digitadores = 35 x 4.000 / 21.100 = 6.6 = 7 Digitadores aproximadamente

Total de equipos de trabajo = 7 puestos de trabajo con su computador y escáner.

El plan de trabajo se llevaría de la siguiente manera:

EL PLAN DE TRABAJO				
ITEM	**TIEMPO POR ITEM**			
	1 MES	**2 MES**	**3 MES**	**4 MES**
1. Compra de Discos Duros	X			
2. Búsqueda del personal pasante de una institución local con pensum en ofimática	X			
3. Búsqueda de los equipo de cómputo en los colegios públicos	X			
4. Revisión de equipos por parte del profesional universitario encargado del área de sistemas	X			
5. Adecuación de la oficina con su parte eléctrica y red separada de la secretaría	X			
6. Capacitación al personal		X		
7. 50% de la digitalización de las hojas de vida			X	
8. 50% restante de digitalización de hojas de vida				X