LINEAMIENTOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – SED

SECRETARÍA DE EDUCACIÓN DEL DISTRITO

BOGOTÁ – COLOMBIA

2023

TABLA DE CONTENIDO

INTRODUCCIÓN....4

1. OBJETIVOS....5

1.1 GENERAL....5

1.2 ESPECÍFICOS....5

2 ALCANCE....6

3 MARCO LEGAL....7

4 TERMINOLOGÍA Y DEFINICIONES....8

5 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA DE EDUCACIÓN DEL DISTRITO....17

6 LINEAMIENTOS DE LOS DOMINIOS DE SEGURIDAD DE LA INFORMACIÓN....18

6.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN....18

6.2 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS....18

6.3 GESTIÓN DE ACTIVOS....19

6.4 CONTROL DE ACCESO....20

6.5 CIFRADO....21

6.6 SEGURIDAD FÍSICA Y AMBIENTAL....21

6.7 SEGURIDAD EN LA OPERACIÓN....22

6.8 SEGURIDAD EN LAS TELECOMUNICACIONES....23

6.9 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN....24

6.10 RELACIONES CON SUMINISTRADORES....25

6.11 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN....25

6.12 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO 25
6.13 CUMPLIMIENTO. 26
7 REVISIONES 27
8 CONTROL DE CAMBIOS 28

INTRODUCCIÓN

La Secretaría de Educación del Distrito SED, considera la información como uno de los activos más importantes para el cumplimiento de la misión institucional; por tal motivo mantiene el compromiso permanente de velar por los principios de seguridad y privacidad de la información, que parte desde la identificación de los riesgos asociados, previniendo, documentando, normalizando y ofreciendo eficiencia, transparencia y accesibilidad a los trámites y servicios ofrecidos por la entidad.

Por lo anterior, la política de seguridad y privacidad de la información de la Secretaría de Educación del Distrito, así como los lineamientos descritos en el presente documento están enmarcados en el modelo de Gobierno y Seguridad Digital, y tiene como principio fundamental la implementación de controles, procesos y estándares que garanticen la disponibilidad, integridad y disponibilidad de los activos de información.

1. OBJETIVOS

1.1 GENERAL

Definir los lineamientos que sirvan para realizar la gestión necesaria hacia la seguridad y privacidad de la información de la Secretaría de Educación del Distrito, identificando y minimizando los riesgos asociados a la información, preservando la integridad, confidencialidad y disponibilidad de la misma, cumpliendo con las normas vigentes en la materia.

1.2 ESPECÍFICOS

- Establecer y velar por el cumplimiento de los principios mínimos generales definidos en las normas vigentes para preservar y mantener la seguridad y privacidad de la información.

- Identificar y mitigar los riesgos en seguridad y gobierno digital para la entidad, así como minimizar los posibles impactos a los servicios que pudieran ser afectados por incidentes, fallas o vulnerabilidades.

- Proteger los activos de la información institucional, mediante la clasificación de controles de acuerdo con los lineamientos de la norma ISO 27002:2013.

2 ALCANCE

La política de seguridad y gobierno digital de la SED aplica a todos los servidores públicos, contratistas, terceros, aprendices, practicantes, usuarios, estudiantes, consultores y en general, a todas las personas que de manera directa o indirecta hagan uso de la información que reserve, administre y trate, a través de la recolección, almacenamiento, intercambio y consultas en el nivel central, local e institucional de la entidad.

A partir de la adopción del Sistema de Gestión de la Seguridad de la Información SGSI en la SED, se realizará seguimiento, gestión, monitoreo y/o auditoría de esta política con base a la norma **ISO/IEC 27001:2013** bajo la guía de controles **ISO/IEC 27002:2013**.

3 MARCO LEGAL

A continuación, se presenta el marco legal que concierne a la política de seguridad y gobierno digital de la SED:

- **Constitución Política de Colombia 1991.** Artículo 15. Reconoce como Derecho Fundamental el Habeas Data.
- **Ley 87 de 1993,** por la cual se dictan Normas para el ejercicio de control interno en las entidades y organismos del Estado, y demás normas que la modifiquen**.**
- **Decreto 1599 de 2005,** por el cual se adopta el Modelo Estándar de Control Interno MECI para el Estado Colombiano.
- **Ley 23 de 1982,** Propiedad Intelectual - Derechos de Autor.
- **Ley 594 de 2000,** Ley General de Archivos.
- **Ley 80 de 1993, Ley 1150 de 2007 y decretos reglamentarios.**
- **Ley 527 de 1999,** por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Ley 1266 de 2008,** por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- **Ley 1273 de 2009,** "Delitos Informáticos" protección de la información y los datos.
- **Ley 1581 de 2012,** "Protección de Datos personales".
- **Decreto 2609 de 2012,** por la cual se reglamenta la ley 594 de 2000 y ley 1437 de 2011.
- **Decreto 1377 de 2013,** por la cual se reglamenta la ley 1581 de 2012.
- **Ley 1712 de 2014,** “De transparencia y del derecho de acceso a la información pública nacional”.
- **Ley 962 de 2005.** “Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas”
- **Ley 1150 de 2007.** “Seguridad de la información electrónica en contratación en línea”
- **Ley 1341 de 2009.** “Tecnologías de la Información y aplicación de seguridad”.
- **Decreto 2952 de 2010.** “Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008”.
- **Decreto 886 de 2014.** “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
- **Decreto 1083 de 2015.** “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”.
- **CONPES 3701 de 2011,** Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **CONPES 3854 de 2016,** Política Nacional de Seguridad digital.
- **CONPES 3995 DE 2020,** Política Nacional de Confianza y Seguridad Digital
- **Norma Técnica Colombiana NTC – ISO/IEC 27000**

4 GLOSARIO

Con el fin de dar definición precisa de los conceptos relacionados en este documento se toman y transcriben los términos estándar relacionados de la norma ISO 27000 de seguridad de la información.[1]

- **Acción correctiva:** Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.
- **Acción preventiva:** Medida de tipo pro-activo orientada a prevenir potenciales no conformidades. Es un concepto de ISO 27001:2005. En ISO 27001:2013, ya no se emplea; ha quedado englobada en Riesgos y Oportunidades.
- **Aceptación del riesgo:** Decisión informada de asumir un riesgo concreto [Fuente: Guía ISO 73: 2009]. La aceptación del riesgo puede ocurrir sin tratamiento de riesgo o durante el proceso de tratamiento de riesgo. Los riesgos aceptados están sujetos a monitoreo y revisión.
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
- **Alcance:** Ámbito de la organización que queda sometido al SGSI.
- **Alcance de auditoría:** Extensión y límites de una auditoría.
- **Alta dirección:** Persona o grupo de personas que dirige y controla una organización al más alto nivel. La alta dirección (o alta gerencia) tiene el poder de delegar autoridad y proporcionar recursos dentro de la organización. Si el alcance del sistema de gestión cubre solo una parte de una organización, la alta dirección se refiere a aquellos que dirigen y controlan esa parte de la organización. A la alta dirección a veces se le llama gerencia ejecutiva y puede incluir directores ejecutivos (CEO), directores financieros (CFO), directores de información (CIO) y funciones similares.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Análisis de riesgos:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. [Fuente: Guía ISO 73: 2009]. El análisis de riesgos proporciona la base para la estimación de riesgos y las decisiones sobre el tratamiento de riesgos. El análisis de riesgos incluye la estimación de riesgos.
- **Análisis de riesgos cualitativo:** Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.
- **Análisis de riesgos cuantitativo:** Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

[1] Recuperado de https://www.iso27000.es/glosario.html en julio 28 de 2020.

- **Ataque:** Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.
- **Auditor:** Persona encargada de verificar, de manera independiente, el cumplimiento de unos determinados requisitos.
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.
- **Autenticación:** Provisión de una garantía de que una característica afirmada por una entidad es correcta.
- **Autenticidad:** Propiedad de que una entidad es lo que afirma ser.
- **Checklist:** Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.
- **Competencia:** Capacidad de aplicar conocimientos y habilidades para lograr los resultados previstos.
- **Compromiso de la Dirección:** Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. La versión de 2013 de ISO 27001 lo engloba bajo la cláusula de Liderazgo.
- **Comunicación y consulta de riesgos:** Conjunto de procesos continuos e iterativos que una organización lleva a cabo para proporcionar, compartir u obtener información y entablar un diálogo con las partes interesadas con respecto a la gestión del riesgo.
  La información puede relacionarse con la existencia, naturaleza, forma, probabilidad, importancia, evaluación, aceptabilidad y tratamiento del riesgo.
  La consulta es un proceso bidireccional de comunicación informada entre una organización y sus partes interesadas sobre un tema antes de tomar una decisión o determinar una dirección sobre ese tema. La consulta es un proceso que impacta en una decisión a través de la influencia en lugar del poder y una aportación a la toma de decisiones, no a la toma conjunta de decisiones.
- **Comunidad de intercambio de información:** Grupo de organizaciones que acuerdan compartir información (una organización puede ser un individuo).
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Conformidad:** Cumplimiento de un requisito.
- **Continuidad de la seguridad de la información:** Procesos y procedimientos para garantizar una operativa continuada de la seguridad de la información.

- **Consecuencia:** Resultado de un evento que afecta los objetivos. [Fuente: Guía ISO 73: 2009]: Un evento puede llevar a una serie de consecuencias. Una consecuencia puede ser segura o incierta y, en el contexto de la seguridad de la información, suele ser negativa. Las consecuencias pueden expresarse cualitativa o cuantitativamente. Las consecuencias iniciales pueden incrementarse a través de los efectos secundarios.
- **Control:** Medida por la que se modifica el riesgo.
  [Fuente: ISO Guide 73:2009] Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. El término salvaguarda o contramedida son utilizados frecuentemente como sinónimos de control.
- **Control correctivo:** Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.
- **Control detectivo**: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.
- **Control de acceso:** Significa garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad.
- **Control disuasorio:** Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención.
- **Control preventivo:** Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.
- **Corrección:** Acción para eliminar una no conformidad detectada. Si lo que se elimina es la causa de la no conformidad, véase acción correctiva.
- **Criterio del riesgo** Términos de referencia contra los cuales se estima la importancia del riesgo [Fuente: Guía ISO 73: 2009].
  Los criterios del riesgo se basan en los objetivos de la organización y el contexto externo y el contexto interno. Los criterios de riesgo pueden derivarse de estándares, leyes, políticas y otros requisitos.
- **Eficacia:** Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.
- **Estimación de riesgos:** Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable. [Fuente: ISO Guide 73:2009]. La estimación de riesgos ayuda en la decisión sobre el tratamiento de riesgos.
- **Evaluación de riesgos:** Proceso global de identificación, análisis y estimación de riesgos. [Fuente: ISO Guide 73:2009]
- **Evento:** Ocurrencia o cambio de un conjunto particular de circunstancias.

[Fuente: ISO Guide 73: 2009]: Un evento puede ser una o más ocurrencias y puede tener varias causas. Un evento puede consistir en que algo no suceda. Un evento a veces puede ser referido como un "incidente" o "accidente".

- **Evento de seguridad de la información:** Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.
- **Evidencia objetiva:** Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión de seguridad de la información.
- **Gestión de claves:** Controles referidos a la gestión de claves criptográficas.
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
- **Gestión de riesgos** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. [Fuente: ISO Guide 73:2009].
  Se compone de la evaluación y el tratamiento de riesgos.
- **Gobernanza de la seguridad de la información:** Sistema mediante el cual las actividades de seguridad de la información de una organización se dirigen y controlan.
- **Hardering:** (palabra en ingles que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc. Innecesarios en el sistema, así como cerrando puertos que tampoco estén en uso. Según el modelo de defensa en profundidad, el host es sólo una capa de éste. En otras palabras, un factor más a considerar dentro del gran número de puntos a ser tomados en cuenta para defender “globalmente” un sistema.
- **Host:** En los sistemas operativos, el término “terminal anfitrión” denota típicamente un ordenador o software que proporciona servicios a múltiples terminales de ordenador o un ordenador que sirve a dispositivos o periféricos (terminales de computo, impresión o video). Es un ordenador que funciona como el punto de inicio y final de las transferencias de datos. También es utilizado como el lugar donde reside un sitio web. Un host de Internet tiene una dirección de Internet única (dirección IP) y un nombre de dominio único o nombre de host.
- **Identificación de riesgos:** Proceso de encontrar, reconocer y describir riesgos [Fuente: Guía ISO 73:2009].
  La identificación de riesgos implica la identificación de las fuentes del riesgo, eventos, sus causas y sus posibles consecuencias. La identificación de riesgos puede involucrar

datos históricos, análisis teóricos, opiniones informadas y de expertos, y las necesidades de las partes interesadas.

- **Impacto:** El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.
- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Indicador:** Medida que proporciona una estimación o evaluación.
- **Información documentada:** Información requerida para ser controlada y mantenida por una organización y el medio en el que está contenida.
  La información documentada puede estar en cualquier formato y medio y desde cualquier fuente y puede referirse al sistema de gestión (incluidos los procesos relacionados), información creada para que la organización funcione (documentación) y/o evidencias de resultados alcanzados (registros).
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.
- **Inventario de activos:** Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
- **ISO:** Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).
- **ISO/IEC 27001:** Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.
- **ISO/IEC 27002:** Código de buenas prácticas en gestión de la seguridad de la información. Primera publicación en 2005; segunda edición en 2013. No es certificable.
- **Mejora continua:** Actividad recurrente para aumentar el rendimiento.
- **Monitoreo:** Determinar el estado de un sistema, un proceso o una actividad. Para determinar el estado, puede ser necesario verificar, supervisar u observar críticamente.
- **Nivel de riesgo:** Magnitud de un riesgo expresado en relación a la combinación de consecuencias y su probabilidad [Fuente: ISO Guide 73: 2009].
- **No conformidad:** Incumplimiento de un requisito.
- **No repudio:** Capacidad de probar la ocurrencia de un evento o acción reclamada y sus entidades de origen.
  Según [CCN-STIC-405:2006]: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación.

Según [OSI ISO-7498-2]: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

- **Objetivo:** Resultado a alcanzar. Un objetivo puede ser estratégico, táctico u operativo. Los objetivos pueden relacionarse con diferentes disciplinas (como las metas financieras, de salud y seguridad y ambientales) y pueden aplicarse a diferentes niveles (como estratégico, de toda la organización, proyecto, producto y proceso). Un objetivo puede expresarse de otras maneras, por ejemplo, como un resultado previsto, un propósito, un criterio operativo, como un objetivo de seguridad de la información o mediante el uso de otras palabras con un significado similar (por ejemplo, propósito, meta o hito).
  En el contexto de los sistemas de gestión de seguridad de la información, la organización establece los objetivos de seguridad de la información, de acuerdo con la política de seguridad de la información, para lograr resultados específicos.
- **Objetivo de control:** Declaración que describe lo que se debe lograr como resultado de la implementación de los controles.
- **Objetivo de la revisión:** Declaración que describe lo que se debe lograr como resultado de una revisión.
- **Organización:** Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos.
  El concepto de organización incluye, pero no se limita a un comerciante individual, compañía, corporación, agencia, empresa, autoridad, sociedad, organización benéfica o institución, o parte o combinación de las anteriores, ya sea sociedad anónima o no, pública o privada.
- **Parte interesada:** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **PDCA:** Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). La actual versión de ISO 27001 ya no lo menciona directamente, pero sus cláusulas pueden verse como alineadas con él.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- **Política:** Intenciones y dirección de una organización, expresada formalmente por su alta dirección.

- **Política de escritorio despejado:** La política de la empresa que indica a los empleados que deben dejar su área de trabajo libre de cualquier tipo de informaciones susceptibles de mal uso en su ausencia.
- **Proceso:** Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.
- **Proceso de gestión del riesgo:** Aplicación sistemática de políticas de gestión, procedimientos y prácticas a las actividades de comunicación, consultoría, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, monitoreo y revisión de riesgos [Fuente: ISO Guide 73: 2009].
  ISO/IEC 27005 utiliza el término "proceso" para describir la gestión de riesgos en general. Los elementos dentro del proceso de gestión de riesgos se denominan "actividades".
- **Profesional del sistema de gestión de seguridad de la información (SGSI):** Persona que establece, implementa, mantiene y mejora continuamente uno o más procesos del sistema de gestión de seguridad de la información.
- **Propietario del riesgo:** Persona o entidad con responsabilidad y autoridad para gestionar un riesgo [Fuente: ISO Guide 73:2009].
- **Recursos de tratamiento de información:** Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.
- **Rendimiento:** Resultado medible. El rendimiento puede relacionarse con hallazgos cuantitativos o cualitativos. El rendimiento puede relacionarse con la gestión de actividades, procesos, productos (incluidos servicios), sistemas u organizaciones.
- **Requisito:** Necesidad o expectativa que es establecida, generalmente de forma implícita u obligatoria.
  “Generalmente implícita” significa que es costumbre o práctica común para la organización y las partes interesadas donde la necesidad o expectativa bajo consideración está implícita. Un requisito especificado es uno que se establece, por ejemplo, en información documentada.
- **Revisión:** Actividad realizada para determinar la idoneidad, adecuación y efectividad del objeto de estudio para lograr los objetivos establecidos [Fuente: ISO Guide 73: 2009].
- **Riesgo:** Efecto de la incertidumbre sobre los objetivos.
  Un efecto es una desviación de lo esperado: positivo o negativo.
  La incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o probabilidad.
  El riesgo a menudo se caracteriza por la referencia a posibles "eventos" (Guía ISO 73: 2009) y "consecuencias" (Guía ISO 73: 2009) o una combinación de estos.
  El riesgo a menudo se expresa en términos de una combinación de las consecuencias de un evento (incluyendo cambios en las circunstancias) y la "probabilidad" asociada (Guía ISO 73: 2009) de ocurrencia.

En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información pueden expresarse como un efecto de incertidumbre sobre los objetivos de seguridad de la información.

El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.

- **Riesgo residual:** El riesgo que permanece tras el tratamiento del riesgo.
  El riesgo residual puede contener un riesgo no identificado. El riesgo residual también puede denominarse "riesgo retenido".
- **Segregación de tareas:** Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.
  Adicionalmente, otras propiedades como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucradas.
- **Selección de controles:** Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.
- **SGSI:** Sistema de Gestión de la Seguridad de la Información.
- **Sistema de Gestión:** Conjunto de elementos interrelacionados o interactivos de una organización para establecer políticas y objetivos y procesos para alcanzar esos objetivos.
  Un sistema de gestión puede abordar una sola disciplina o varias disciplinas. Los elementos del sistema incluyen la estructura, roles y responsabilidades, planificación y operación de la organización. El alcance de un sistema de gestión puede incluir la totalidad de la organización, funciones específicas e identificadas de la organización, secciones específicas e identificadas de la organización, o una o más funciones en un grupo de organizaciones.
- **Sistema de Gestión de la Seguridad de la Información:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
- **Sistema de Información:** Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes que manejan información.
- **Statement of Applicability SoA:** Declaración de aplicabilidad.
- **Tratamiento de riesgos:** Proceso para modificar el riesgo [Fuente: Guía ISO 73: 2009].
  Las acciones de tratamiento del riesgo pueden contemplar:

- evitar el riesgo al decidir no comenzar o continuar con la actividad que da lugar al riesgo;
- asumir o aumentar el riesgo para aprovechar una oportunidad;
- eliminar la fuente de riesgo;
- modificar la probabilidad;
- modificar las consecuencias;
- compartir el riesgo con otra parte o partes (incluidos contratos y financiación del riesgo);
- retener el riesgo mediante una elección informada.

Las acciones de tratamiento del riesgo sobre consecuencias negativas a veces se denominan "mitigación de riesgos", "eliminación de riesgos", "prevención de riesgos" y "reducción de riesgos".

El tratamiento del riesgo puede crear nuevos riesgos o modificar los riesgos existentes.

- **Trazabilidad:** Según [CESID:1997]: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA DE EDUCACIÓN DEL DISTRITO

La Secretaría de Educación del Distrito SED, adopta el Modelo de Seguridad y Privacidad de la Información y mediante la resolución 1944 del 27 de octubre de 2016 adopta la Política de Seguridad de la Información, que en sus objetivos estratégicos se compromete a organizar, planificar, implementar, soportar, operar, evaluar y mejorar la Seguridad de la Información de la entidad, a fin de proteger, preservar y asegurar la integridad, confidencialidad y disponibilidad de los activos de información que soportan los procesos de la SED.

6 LINEAMIENTOS DE LOS DOMINIOS DE SEGURIDAD DE LA INFORMACIÓN

6.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

Objetivo de Control: 6.1 Organización Interna.

La Secretaría de Educación del Distrito, define y adopta la implementación, gestión y operación del Sistema Integrado de Gestión en el cual está contenido el Subsistema de Gestión de Seguridad de la Información; definiendo roles y responsabilidades de las personas, áreas y demás que intervengan en los activos de información de la entidad, para minimizar los riesgos de oportunidad frente al uso indebido o modificación no autorizada de los activos con los que dispone la SED.

Objetivo de Control: 6.2 Dispositivos Móviles y de Trabajo

La SED a través de la Oficina de las Tecnologías de la Información y las Comunicaciones, debe implementar el procedimiento que oriente a todas las dependencias de la entidad, acercade la autorización, configuración y uso de cualquier dispositivo móvil que requieran tener acceso a la información mediante las redes de la entidad.

Así mismo dentro de este objetivo, se debe llevar una lista de chequeo del inventario actualizado con los dispositivos autorizados para acceder a la red de la entidad, al igual que se debe implementar las medidas necesarias para garantizar la protección, privacidad y seguridad de la información de la SED.

A través de la Dirección de Talento Humano, se debe establece el procedimiento de teletrabajo y trabajo remoto (este último en el marco de la pandemia por la enfermedad COVID-19) manteniendo los aspectos relacionados con la seguridad y privacidad de la información, dirigido a los teletrabajadores y aspirantes a esta modalidad en la entidad.

6.2 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

Objetivo de Control: Previo al inicio de la Contratación.

Desde la Dirección de Talento Humano, se debe contar con el procedimiento para la verificación del personal de carrera y provisional desde la postulación del cargo, teniendo en cuenta los dictámenes legales y lo mandado por el Departamento Administrativo de la Función Pública.

Desde la Dirección de Contratos, se debe contar con los lineamientos para la revisión de los antecedentes del personal a contratar por prestación de servicios de acuerdo con la legislación vigente.

Objetivo de Control: Durante la Contratación.

Una vez formalizada la vinculación, se debe llevar a cabo el procedimiento descrito para el acceso a los servicios que requiera el usuario y su respectivo inventario que conlleven a la ejecución de las labores asignadas; así mismo, la sensibilización de lo relacionado con el Modelos de Seguridad y Privacidad de la Información por parte de la Oficina de las Tecnologías de la Información y las Comunicaciones en el marco de la inducción programada por la Dirección de Talento Humano.

Objetivo de Control: Cese o cambio de puesto de trabajo.

En el momento de existir alguna novedad relacionada de retiro, inhabilidad, investigación, cambio de función u otras, el jefe de área o a quien este delegue, deberá salvaguardar la información propia de la entidad, en el caso de los contratistas en terminación de contrato anticipada, temporal, cesión del contrato u otras, aplicara el mismo procedimiento de salvaguardar la información. Lo relacionado a información física con procedimiento de archivo de gestión y archivo histórico por parte de la dependencia atendiendo lineamientos y tablas de retención documental establecidas por equipo de Archivo de la Dirección de Servicios Administrativos; y lo relacionado a información digital mediante solicitud de la dependencia a soportesed@educacionbogota.gov.co atendiendo los lineamientos establecidos por la Oficina de las Tecnologías de la Información y las Comunicaciones.

6.3 GESTIÓN DE ACTIVOS

Objetivo de Control: Responsabilidad sobre los activos.

La SED establece mediante la gestión de riesgos la metodología para la actualización de activos de información y define los procedimientos claros para que los usuarios realicen la entrega de los activos que tienen a cargo propiedad de la entidad.

Objetivo de Control: Clasificación de la Información.

La SED cuenta con las Tablas de Retención Documental, las cuales indican el tipo de clasificación (series, subseries y documentos contenidos) y, servirá para los intercambios de información debido a los términos de confidencialidad.

Objetivo de Control: Manejo de los soportes de almacenamiento.

La SED tiene definidos los controles para la gestión de medios de soporte removibles y fijos digitales, la disposición final de los mismos en forma segura y la protección contra acceso no autorizado, uso indebido o corrupción durante la transferencia.

6.4 CONTROL DE ACCESO

Objetivo de Control: Requisitos de negocio para el control de acceso.

La SED a través de la Oficina de las Tecnologías de la Información y las Comunicaciones OTIC, establece los procedimientos mínimos para otorgar el acceso requerido a la red internay sistemas de información con los que se haya solicitado autorización.

Se cuenta con la segregación de redes separando los de servicios con los usados normalmente por los usuarios.

Objetivo de Control: Gestión de acceso al usuario.

La SED a través de la Oficina de las Tecnologías de la Información y las Comunicaciones OTIC, define los lineamientos para la solicitud de creación o cancelación de las cuentas de usuarios mediante los formatos aprobados por la dirección.

La SED vela por que la autenticación de los usuarios sea realizada de manera confidencial, cumpliendo los parámetros establecidos para la asignación de contraseñas y protocolos de conexión seguros

Objetivo de Control: Responsabilidades del usuario.

De acuerdo con lo definido en las recomendaciones mínimas para cambio de contraseñas seguras, los usuarios deberán cumplir a cabalidad con lo descrito, el cambio de contraseñas solo podrán solicitarlo el usuario titular, el jefe o supervisor asignado

Objetivo de Control: Control de acceso a sistemas y aplicaciones.

La SED restringe y controla el uso de programas que puedan anular, bloquear o interceptar la información de los sistemas y controlar el acceso a los códigos fuente de los programas.

La implementación de controles para el acceso a los ambientes de desarrollo, accesos limitado y/o controlado de la información contenida en los ambientes de producción.

6.5 CIFRADO

Objetivo de Control: Controles criptográficos.

La SED garantiza que cualquier sistema de información que requiera transferencia de información cuente con las herramientas de cifrado y encriptación de datos, así como los servicios que lo requieran para proteger la confidencialidad, autenticidad e integridad de la información de la Entidad.

6.6 SEGURIDAD FÍSICA Y AMBIENTAL.

Objetivo de Control: Áreas seguras.

La SED dispondrá de los recursos y acciones que se requieran para garantizar la protección de los sitios seguros donde se encuentren los equipos y elementos, para reducir las amenazas, accesos no autorizados y riesgos ambientales, además de contar con los elementos que minimicen las amenazas que afectan la infraestructura en cuestión de fallas de potencia e interrupciones causadas por los servicios públicos.

Los puntos de accesos deberán contar con vigilancia y demás medios pertinentes para controlar el acceso a los sitios seguros.

Los ingresos a los Data Center y cuartos de cableado estructurado, deberá ser informado al personal de vigilancia, diligenciar la minuta y portar su identificación visible en todo momento; en caso de ser personal externo a la entidad, deberá estar acompañado en todo momento por el personal autorizado de la SED.

Objetivo de Control: Seguridad de los equipos.

Los equipos de cómputo, impresoras y demás elementos tecnológicos están situados en las áreas que reduzcan el riesgo de amenaza ambiental al igual del acceso no autorizado a los mismos.

Aplicar las medidas de seguridad a los activos que se encuentran fuera de los predios de la Secretaría de Educación del Distrito, diferenciando los distintos riesgos de trabajar fuera de

dichos predios, tales como dispositivos móviles, equipos o sistemas en tercerización en modalidad de servicio (SaaS, IaaS, PaaS, hosting, colocación, entre otras).[2]

La SED hace disposición final segura y controla la reutilización de equipos, verificando que todos los elementos que contengan medios de almacenamiento sean retirados o borrados y según el caso destruidos, para asegurar que cualquier dato confidencial o software con licencia no sea expuesto a un riesgo de seguridad.

6.7 SEGURIDAD EN LA OPERACIÓN

Objetivo de Control: Responsabilidades y procedimientos de operación.

La SED mantiene documentados todos los procesos, procedimientos y manuales los cuales están a disposición de todos los usuarios.

Todos los cambios referentes a procesos, infraestructura e instalaciones son controlados y se previene cualquier afectación a la disponibilidad, integridad y confidencialidad de la información.

Objetivo de Control: Protección contra código malicioso.

La SED mediante la Oficina de las Tecnologías de la Información y las Comunicaciones OTIC realiza campañas de sensibilización a los usuarios sobre los riesgos provenientes de códigos maliciosos.

La SED mantiene actualizada la base de datos correspondiente a firmas y parches de seguridad en el software de antivirus y demás elementos tecnológicos de seguridad perimetral.

La entidad implementa procedimientos para controlar la instalación de software en sistemas operativos, obtiene información acerca de las vulnerabilidades técnicas de los sistemas de información.

Objetivo de Control: Copias de seguridad.

La entidad implementa y documentas procesos eficaces, eficientes y controlados para la gestión de las copias de respaldo de la información, software e imágenes de los sistemas y pone a prueba regularmente la capacidad de recuperación.

[2] infraestructura como servicio (**IaaS**), plataforma como servicio (**PaaS**) y software como servicio (**SaaS**) por sus siglas en inglés

Objetivo de Control: Registro de actividad y supervisión.

La SED genera registros de auditoría y huella digital los cuales documentan los eventos relacionados a la seguridad en todos los sistemas de información.

Se lleva a cabo el proceso de monitoreo de perfiles y roles para garantizar que los usuarios accedan para las actividades asignadas a su labor definida.

Objetivo de Control: Control del software en explotación.

La Oficina de las Tecnologías de la Información y las Comunicaciones OTIC deberá llevar registro y control de los programas propios de la entidad referente a software de producción, librerías y actualizaciones de los mismos, así como la documentación de cada sistema.

Objetivo de Control: Gestión de la vulnerabilidad técnica.

La SED deberá implementar procedimientos que permitan controlar la instalación de software no autorizado en los sistemas operativos, evitando vulnerabilidades técnicas que afecten los sistemas de información, además de evaluar la exposición de la entidad frente a vulnerabilidades expuestas tomando las medidas necesarias para tratar el riesgo.

Objetivo de Control: Consideraciones de las auditorias de los sistemas de información.

La SED deberá implementar mejores prácticas para establecer políticas sobre las auditorias de todo el sistema de gestión de seguridad y privacidad de la información.

6.8 SEGURIDAD EN LAS TELECOMUNICACIONES.

Objetivo de Control: Gestión de la seguridad en redes.

Mediante los equipos perimetrales y de seguridad la SED tiene segmentos de red en los cuales separa los servicios de internet, de usuarios, terceros y sistemas de información.

Con el fin de evitar accesos no autorizado, se mantienen cerrados, bloqueados y en monitoreo de seguridad los puertos de configuración y diagnostico asignados únicamente a los sistemas de información.

Se tendrá deshabilitado las opciones del protocolo IPv6 si no se está usando por la entidad.

Se realiza permanente hardening en dispositivos de red.

Objetivo de Control: Intercambio de información con partes externas.

La SED deberá revisar periódicamente los procedimientos que ofrecen seguridad en la información que se transfiere con el fin de evitar la integridad y confidencialidad.

La entidad revisa los acuerdos de confidencialidad y no divulgación de acuerdo a las necesidades puntuales y conforme a lo estipulado en la ley.

6.9 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

Objetivo de Control: Requisitos de seguridad de los sistemas de información.

La SED realiza la documentación y define los requisitos de seguridad, los cuales deben cumplir todos los sistemas de información de le entidad, aplica tanto para el uso interno como externo, así como el utilizado por terceros.

Se estandarizan los requerimientos, normas y procedimientos para nuevos sistemas de información, al igual que las modificaciones requeridas en los sistemas ya existentes, de manera que se tenga en cuenta el análisis y posterior implementación de acuerdo con la seguridad del sistema.

Objetivo de Control: Seguridad en los procesos de desarrollo y soporte.

La SED deberá orientar sobre las buenas prácticas de seguridad frente al desarrollo de software, contar con un control de versiones y tener la capacidad de identificar, evitar y solucionar vulnerabilidades.

Se realiza permanente hardening en las aplicaciones o desarrollos que lo permiten.

Mediante el control de versiones de los sistemas de información, se deberá identificar los puntos anteriores de los mismos para poder reutilizar el código si es necesario.

Contar con el o los controles de cambio de los sistemas de información que permitan ser documentados para así garantizar la integridad desde el levantamiento de requerimientos, etapa de diseño y posteriores mantenimientos.

Objetivo de Control: Datos de prueba.

La SED controla y limita el acceso a los ambientes de prueba y producción de los sistemas de información, velando que los datos utilizados de prueba no contengan información sensible en los ambientes de prueba de los aplicativos.

6.10 RELACIONES CON SUMINISTRADORES.

Objetivo de Control: Seguridad de la información en las relaciones con suministradores.

La SED establece los lineamientos pertinentes de seguridad de la información frente a las obligaciones contractuales de los terceros, define los compromisos de confidencialidad mediante acuerdos ajustados a cada necesidad.

Se debe establecer en los contratos los temas legales y regulatorios de acuerdo a la confidencialidad y cumplimiento de la política de seguridad de la información de la SED.

Objetivo de Control: Gestión de la prestación del servicio por suministradores.

La SED deberá controlar los servicios ofrecidos por los proveedores frente a cualquier cambio en los servicios ofrecidos, los mantenimientos, velando por las políticas de seguridad, la criticidad de la información, sistemas y procedimientos que involucren cualquier riesgo asociado.

6.11 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

Objetivo de Control: Gestión de incidentes de seguridad de la información y mejoras

La SED establecerá los lineamientos para asegurar que se reciba la información relacionada con incidentes de seguridad y sea administrada de forma eficaz, mediante los canales de comunicación de gestión apropiados, indicados a los usuarios en general.

Los usuarios deberán informar o reportar cualquier evento o sospecha de incidentes relacionados con la seguridad de la información para así, contrarrestar las interrupciones o vulnerabilidades generadas a los sistemas e infraestructura de la Entidad.

6.12 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

Objetivo de Control: Continuidad en la seguridad de la información.

Se deberá proyectar y diseñar la metodología apropiada para la entidad, la cual identifique y evalúen los riesgos asociados a la continuidad de la operación de la Secretaría de Educación del Distrito.

Realizar el análisis enfocado a la identificación de los servicios críticos de la SED.

Diseñar la metodología para el plan de recuperación de desastres de la operación de la Secretaría de Educación del Distrito.

Objetivo de Control: Redundancias.

Se cuenta con la disposición de las instalaciones de la entidad, para el debido procesamiento de la información cumpliendo con los requisitos de disponibilidad, mediante la redundancia suficiente.

6.13 CUMPLIMIENTO.

Objetivo de Control: Cumplimiento de los requisitos legales y contractuales.

De acuerdo con las obligaciones legales, normativas, estatutarias y/o contractuales, la SED establecerá los lineamientos para dar cumplimiento a los requisitos descritos en materia de seguridad y privacidad de la información.

La SED garantiza la protección y privacidad de la información personal y datos sensibles establecidos en la ley.

Objetivo de Control: Revisiones de la seguridad de la información.

Mediante el Comité técnico del Subsistema de Gestión de la Seguridad de la Información establece la revisión del cumplimiento de los procesos establecidos con las políticas, lineamientos y manuales de la seguridad y privacidad de la información.

7 REVISIONES

Los lineamientos de la política de seguridad y privacidad de la información de la Secretaría de Educación del Distrito, se revisará periódicamente y se realizaran las actualizaciones pertinentes, relacionado con cada control a partir de la declaración de aplicabilidad de los controles en la norma, de acuerdo con lo propuesto por las políticas de Gobierno Digital y Seguridad Digital.

8 CONTROL DE CAMBIOS

No. Ver.	Fecha Ver.	Elaborado por	Revisado por	Aprobó	Descripción
V.1.0.	mar-2021	Duber Jair Rocha Henry Alexander Moyan	Equipo de gobierno y seguridad digital	Wilson Adiel Rodriguez Rodriguez	Emisión Política .
V.2.0	Nov-2023	Julio Andrés Sánchez	Equipo de gobierno y seguridad digital	Wilson Adiel Rodriguez Rodriguez	Actualización Política

Proyectó: Henry Alexander Moyan Montenegro – Profesional Contratista OTIC
Julio Andrés Sánchez - Profesional Especializado Contratista OTIC

Revisó: Equipo Gobierno y Seguridad Digital

Aprobó: Wilson Adiel Rodríguez Rodríguez – Líder de la Política de Gobierno y Seguridad Digital