Contenido

MODELO DE SEGURIDAD Y PRIVACIDAD DIGITAL (MSPI)

INSTITUTO COLOMBIANO DE CRÉDITO EDUCATIVO Y ESTUDIOS TÉCNICOS EN EL EXTERIOR MARIANO OSPINA PÉREZ - ICETEX

TABLA DE CONTENIDO

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

El Modelo de Seguridad y Privacidad Digital del Icetex (MSPI en adelante) es la guía para establecer, implementar, mantener y mejorar el Sistema de Gestión de Seguridad Digital del Instituto y describe los componentes requeridos para la administración razonable de la seguridad y privacidad de la información.

Es la herramienta que permite administrar el Sistema de Gestión de Seguridad Digital. Sistemáticamente el modelo articula una serie de elementos orientados para entregar servicios a las áreas misionales, de apoyo y estratégicas en términos de consolidar la confianza en los grupos de interés internos y externos del Instituto.

El Sistema de Gestión de Seguridad Digital ha sido construido tomando como base las directrices del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de la Tecnologías de la Información y las Comunicaciones, de acuerdo con las necesidades propias del Instituto.

El Icetex adopta el presente Modelo de Seguridad y Privacidad Digital con el propósito de fortalecer la protección de los activos de información, atendiendo los lineamientos de la Política de Gobierno Digital en el uso y aprovechamiento de las tecnologías de la información y comunicaciones, en atención al marco del artículo 2.2.9.1.1.2. del Decreto 1078 de 2015 (DUR-TIC).

2. DEFINICIONES Y TÉRMINOS

- **Activo de información:** se refiere a cualquier información o elemento relacionado que tenga valor para la organización y por lo tanto debe protegerse. (Definición tomada de la norma ISO27001:2013). En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital y física. (Definición tomada Guía para la administración del riesgo y el diseño de controles en entidades públicas).
- **Activo**: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
- **Activos de Información y recursos**: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 20116).
- **Archivo**: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).
- **Amenazas**: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO 2700/IEC 27000).
- **Análisis de riesgo de seguridad digital:** proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.
- **Auditoría:** proceso sistemático, independiente y documentado para obtener evidencias de auditoría y determinar el grado en el que se cumplen los criterios establecidos (ISO/IEC 27000).
- **Autorización de tratamiento de datos personales**: consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos (Ley 1581 de 2012, art 3°).
- **Bases de Datos Personales**: conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).
- **Ciberamenaza:** aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.
- **Ciberataque**: acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de comisión de un crimen.
- **Ciberseguridad**: es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la Entidad.
- **Ciberespacio**: es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Control:** es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.
- **Control Preventivo:** están diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos.
- **Control Detectivo:** están diseñados para identificar un evento o resultado no previsto después de que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes.
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Declaración de aplicabilidad:** es el documento que enumera los controles aplicados por el Modelo de Seguridad y Privacidad Digital de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del Anexo A de NTC-ISO-IEC 27001.
- **Gestión de incidentes de seguridad digital:** son las actividades para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad digital (ISO/IEC 27000).
- **Información Pública:** es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

- **Información Pública Clasificada**: es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Información Pública Reservada:** es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Mecanismos de protección de datos personales**: lo constituyen las distintas alternativas con que cuentan las Entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

- **Plan de continuidad del negocio:** plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- **Plan de tratamiento de riesgos:** es el documento que define las acciones para gestionar los riesgos de seguridad digital inaceptables e implementar los controles necesarios para protegerla (ISO/IEC 27000).

- **Riesgo:** es la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 27000).

- **Seguridad de la información:** es la preservación de la confidencialidad, integridad y disponibilidad de la información en cualquier medio: impreso o digital (ISO/IEC 27000).

- **Sistema de Gestión de Seguridad Digital (SGSD):** es el conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que una organización utiliza para establecer una política y unos objetivos de seguridad de la información y alcanzarlos, basándose en un enfoque de gestión y de mejora continua (ISO/IEC 27000).

- **Seguridad digital**: preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

- **Software**: para efectos del presente modelo se entiende por software las aplicaciones, motores de bases de datos, sistemas operativos y demás componentes lógicos de computación utilizadas para la operación en el Icetex.

- **Titulares de la información**: personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

- **Tratamiento de Datos Personales**: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

- **Trazabilidad:** es la cualidad que permite que todas las acciones realizadas sobre la información, o sobre un sistema de tratamiento de la información, sean asociadas de modo inequívoco a un individuo o Entidad (ISO/IEC 27000).

- **Vulnerabilidad:** son las debilidades, brechas de seguridad o falencias inherentes a los controles de seguridad sobre los activos de información que pueden ser explotadas por factores externos y no controlables por el Instituto (amenazas), las cuales se constituyen en fuentes de riesgo.

- **Parte interesada (*stakeholder*):** es la persona u organización que puede afectar, ser afectada o percibirse a sí misma como afectada por una decisión o actividad.

3. PROPÓSITOS

- Aportar en el desarrollo e implementación de la estrategia de seguridad digital en el Icetex.

- Contribuir en el desarrollo y ejecución del plan estratégico institucional, de cada entidad, a través de los planes de seguridad y privacidad de la información.

- Establecer procedimientos de seguridad que permitan a las Entidades apropiar el habilitador de seguridad en la política de Gobierno Digital.

4. MARCO JURÍDICO

Las siguientes son las referencias normativas aplicables a la seguridad digital de la Entidad:

- Artículos 15, 209 y 269 de la Constitución Política de Colombia.
- Ley 527 de 1999 - Acceso y uso de los mensajes de datos.
- Ley 1273 de 2009 – Delitos informáticos.
- Ley 1341 de 2009 establece que el Gobierno Nacional fijará los mecanismos y condiciones para garantizar la masificación del Gobierno en Línea, en lo referente a Protección de los derechos de los usuarios.
- Ley 1221 de 2008 - Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- Decreto 884 de 2012- restricciones de uso de equipos y programas informáticos y regulación de Teletrabajo.
- Ley 1581 de 2012– Protección de Datos Personales.
- Ley 1712 de 2014– Transparencia y Derecho de Acceso a la Información Pública.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Ley 2088 de 2021. Por la cual se regula el trabajo en casa y se dictan otras disposiciones.
- Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario.
- Decreto 2364 de 2012. Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del

Estado.

- Decreto 2106 de 2019, establece la disposición de una estrategia de seguridad digital acorde con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones- MInTic.
- Decreto 1377 de 2013 (Compilado en el Decreto 1081 de 2015), por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 103 de 2015, por el cual se reglamenta parcialmente la Ley 1712 de 2014 y el acceso a la información pública.
- Decreto 886 de 2014, Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
- Decreto 1008 de 2018 – Política de Gobierno Digital (MinTIC).
- Decreto 25 de agosto de 2017: los lineamientos que se deben cumplir para la prestación de servicios ciudadanos digital.
- Decreto 620 de 2020: estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- Decreto 338 de 2022, contiene lineamientos generales para fortalecer la gobernanza de la seguridad digital.
- Superintendencia Financiera de Colombia:
    - Circular Básica Jurídica 029 de 2014 Parte 1, Título II, Capítulo I – Canales, medios, seguridad y calidad en el manejo de información de prestación de servicios financieros,
    - Circular Básica Jurídica 029 de 2014 Parte 1, Título IV, Capítulo V – Requerimientos mínimos para la gestión del riesgo de ciberseguridad
    - Circular Básica Jurídica 029 de 2014 Parte 1, Título I, Capítulo VI – Reglas relativas al uso de servicios de computación en la nube.
    - Circular Externa 033 de 2020. Instrucciones relacionadas con la Taxonomía Única de Incidentes Cibernéticos – TUIC, el formato para el reporte de métricas de seguridad de la información y ciberseguridad y el protocolo de etiquetado para el intercambio de información Traffic Light Protocol (TLP).
- MINTIC: Modelo de Seguridad y Privacidad Digital (MSPI) de la Estrategia de Gobierno Digital.
- NTC-ISO-IEC 27001 – norma técnica colombiana – Sistema de Gestión de Seguridad de la Información.
- Modelo Integrado de Planeación y Gestión – Dimensión Seguridad Digital.
- CONPES 3854 de 2016 Política Nacional de Seguridad digital
- CONPES 3995 de 2020 - Política Nacional de Confianza y Seguridad Digital.
- Directiva presidencial 03 de 2021. Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
- Directiva presidencial 02 de 2022. Lineamientos para el uso de servicios en la nube, actualización de catálogos de servicios, sistemas de información, bases de datos, activos de información, infraestructura; Implementar una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos, conformación de un equipo o Grupo de Seguridad Digital.
- Resolución 500 de 2021. “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”
- Resolución 1519 de 2020. Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos”.
- Resolución 460 de 2022 “Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación”.
- Circular 018 de 2021. Procuraduría General de la Nación. Implementación de la Resolución 1519 de 2020.

5. DIAGNÓSTICO

El Icetex tiene implementado realizar un diagnóstico anual mediante el “Instrumento de Evaluación MSPI”, donde se identifica el nivel de madurez de la seguridad y privacidad y posibles acciones tendientes a la mejora continua de la seguridad digital.

6. COMPOSICIÓN DEL MSPI

El Modelo de Seguridad y Privacidad Digital está conformado por los siguientes elementos:

Gráfico 1: *Arquitectura del Modelo de Seguridad y Privacidad Digital del Icetex*

La arquitectura del modelo asegura que en todo el tiempo se opere la seguridad digital con un enfoque en los objetivos institucionales, la gestión de necesidades y expectativas de las partes interesadas, ello auspiciando la construcción y entrega de servicios de alto valor alineados a la estrategia innovadora y sostenible del Instituto. Los insumos esenciales para la operación del modelo son la estrategia y objetivos del Instituto, que se complementan con políticas, procedimientos y controles técnicos y manuales que proporcionan un marco estructurado para el control de los riesgos de seguridad digital.

Los elementos del gráfico 2, muestra como el MSPI se opera bajo un modelo PHVA (Planear – Hacer- Verificar -Actuar), contiene los elementos específicos enfocadas en mantener al Sistema de Gestión de Seguridad Digital y los conforman:

La Planeación o Planificación está compuesta por cuatro (4) partes, ellas son:

Conocimiento organizacional
Liderazgo
Planificación
Soporte

La Operación la conforma el plan de implementación de controles y el seguimiento de implementación de controles. Los controles se definen de los requerimientos del Anexo A de la Norma ISO27001:2013 así como de la demás normativa existente en la materia, así como de las mitigaciones que se selecciones para proteger los activos de información en los procesos de la Entidad.

Evaluación del MSPI: El plan de evaluación y monitoreo contempla las acciones necesarias para el evaluar el desempeño y la eficacia del Sistema de Gestión de Seguridad Digital, la cual se desarrolla a partir de indicadores, planificación de las acciones de medición, seguimiento y evaluación de estos.

La Mejora Continua: mediante la mejora continua se evalúa la necesidad de tomar acciones para eliminar causas potenciales de situaciones que puedan afectar el sistema de gestión de seguridad digital. Estas acciones garantizar su adecuación y eficacia durante todo su ciclo PHVA (planear, hacer, verificar y actuar).

El detalle del Modelo de Seguridad y Privacidad Digital - MDPI se define en los siguientes aspectos:

7. PLANIFICACIÓN

Con base en el autodiagnóstico, el Icetex elabora el Plan de Seguridad y Privacidad de la Información con el objeto de disponer de la planeación del tiempo, recursos y presupuesto de las actividades que va a desarrollar relacionadas con el MSPI, está conformado por:

7.1. CONTEXTO DE LA ENTIDAD

El Icetex realiza el entendimiento de la organización a través del análisis de su contexto interno y externo de seguridad digital, la identificación de las partes interesadas junto con sus necesidades y expectativas y define el alcance del Sistema de Gestión de Seguridad Digital.

7.1.1. CONOCIMIENTO DE LA ORGANIZACIÓN Y CONTEXTO

CONOCIMIENTO DE LA ORGANIZACIÓN

El propósito es | detalle las características del Icetex y su entorno, para permitir implementar el MSPI adaptado a las condiciones específicas, para ello determina los aspectos externos e internos que son relevantes con las actividades que realiza la Entidad en el desarrollo de su misión y que podrían influir en las capacidades para lograr los objetivos del modelo, alineado con los objetivos estratégicos.

El Icetex es una entidad financiera de naturaleza especial, con personería jurídica, autonomía administrativa, y patrimonio propio, vinculada al Ministerio de Educación Nacional, creado por el Decreto 2586 de 1950 y transformado por la Ley 1002 del 30 de diciembre de 2005. Tiene por objeto el fomento social de la educación superior, priorizando en la población de bajos recursos económicos y aquella con mérito académico en todos los estratos, a través de mecanismos financieros que hagan posible el acceso y la permanencia de las personas a la educación superior, la canalización y administración de recursos, becas y otros apoyos de carácter nacional e internacional, con recursos propios o de terceros. Para cumplir con su objeto, la Entidad ha establecido criterios de cobertura, calidad y pertinencia educativa, en condiciones de equidad territorial; igualmente otorga subsidios para el acceso y permanencia en la educación superior de los estudiantes de estratos 1, 2 y 3.

- **PROPÓSITO SUPERIOR**

Impulsamos proyectos de vida brindando las mejores alternativas para crear caminos incluyentes en la educación superior.

- **VISIÓN**

Ser la primera opción de los colombianos para el acceso y permanencia en la educación superior a través de servicios agiles, flexibles, sostenibles y con enfoque diferencial.

- **MAPA DE PROCESOS**

De acuerdo con la arquitectura de procesos, el Icetex ha definido 5 macroprocesos misionales para satisfacer las necesidades de los clientes, 8 macroprocesos para soportar la ejecución de los procesos misionales, 2 macroprocesos estratégicos y uno (1) de evaluación. Dichos procesos se muestran en el gráfico 1.

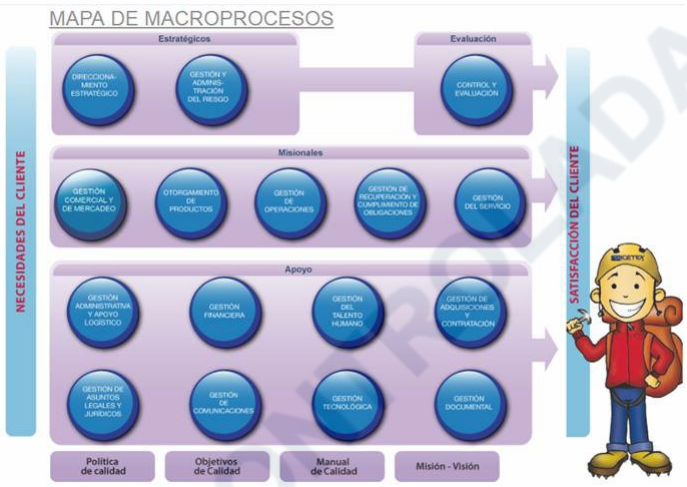

***Gráfico 2**: Mapa de Macroprocesos del ICETEX*

CONTEXTO DE LA ENTIDAD

El Icetex como parte del Gobierno Nacional, se ve influenciado principalmente por los impactos de la economía nacional, el orden social, normativo en el marco de seguridad digital y los lineamientos futuros en materia de desarrollo de la educación superior o regulación del sector financiero.

Basado en lo anterior, se actualiza de manera periódica su contexto de seguridad digital para incorporar los cambios en directrices de Ministerio de la Tecnologías de la Información y las Comunicaciones, de la Superintendencia Financiera de Colombia, los lineamientos de Modelo Integrado de Gestión Pública del Departamento Administrativo de Función Pública – DAFP y el análisis del entorno de operación de sus servicios.

A continuación, se describen los principales factores internos y externos que pueden afectar la seguridad digital del Icetex:

INTERNAS	EXTERNAS
La dependencia de los proveedores críticos.	Cambio de Normatividad legal en el ámbito nacional o internacional en cuanto a seguridad digital.
El software misional desactualizado o no es escalable conforme a la actualización tecnológica.	Políticas sectoriales suministradas por el Ministerio de Educación Nacional y Ministerio de Hacienda.
Alta rotación de personal que afecta la continuidad de los procesos.	Aspectos sociales, culturales, políticos, legales, reglamentarios, financieros, tecnológicos, económicos, naturales y competitivo, ya sea internacional, nacional, regional o local.
Gobierno de la Entidad y estructura organizacional, funciones y rendición de cuentas.	Directrices clave y tendencias que tengan impacto en los objetivos estratégicos de la organización.
Las políticas, los objetivos y las estrategias que existen para lograrlos.	Relaciones, percepciones y valores de las partes interesadas externas.
Capacidades, entendidas en términos de recursos y conocimientos (por ejemplo, capital, tiempo, personas, procesos, sistemas y tecnologías).	Creciente aumento de las amenazas informáticas, ciberataques, hacktivismo, ciber inteligencia, que se pueden aprovechar de la situación en confinamiento y trabajo remoto.
Relaciones, percepciones y valores de los actores internos y la cultura de la organización.	Niveles generales de confianza y credibilidad de los clientes.
Sistemas de información, flujos de información y procesos de toma de decisiones.	Dinámica macroeconómica del estado colombiano.
Normas, directrices y modelos adoptados por la entidad.	Políticas y directrices gubernamentales en materia de promoción de la educación superior.
Forma y alcance de las relaciones contractuales.	Percepción de los clientes de los productos del Instituto sobre su calidad, oportunidad o facilidad de acceso.

INTERNAS	EXTERNAS
Uso de equipos de cómputo personales sin los adecuados mecanismos de protección y ausencia de buenas prácticas por parte del usuario.	Adopción de nuevas formas de interacción con el ciudadano (redes sociales), innovaciones tecnológicas que aún no cuentan con marcos legales claros (criptomonedas, billeteras virtuales, herramientas colaborativas como WhatsApp).
La necesidad de intercambiar información con terceras partes (aliados estratégicos, proveedores y entes de control) para el cumplimiento de los objetivos estratégicos	Transparencia y acceso a la información pública.
Cultura organizacional frente a la protección de la Información y la seguridad digital	Infraestructura crítica cibernética.

Tabla 1. *Factores que pueden afectar la Seguridad Digital*

7.1.2. NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

El Icetex identifica las partes interesadas internas o externas como las personas, entidades u organizaciones que pueden influir directamente en la seguridad y privacidad de la información de la Entidad o que pueden ser afectados en caso de que estas se vean comprometidas, en complemento, determina sus necesidades y expectativas (intereses) relacionados con la seguridad y privacidad de la información.

Las necesidades y expectativas de las partes interesadas van enfocadas a que se les asegure la confidencialidad, integridad y disponibilidad de la información mediante la adopción del Sistema de Gestión de Seguridad Digital acorde con la Estrategia de Gobierno Digital. La Entidad reconoce las siguientes como partes interesadas:

- **Funcionarios:** Trabajadores con contrato laboral con la Entidad o personas en calidad de pasantes.
- **Beneficiarios, Becario, participantes de programas:** Personas que requieran financiar sus estudios universitarios, deudores solidarios y personas que acceden a becas gestionadas por el Instituto.
- **Ciudadanos:** Personas interesadas en los servicios y productos que promulga el Icetex, así como personas veedoras de la gestión y políticas de la Entidad.
- **Aliados Estratégicos:**
  - Entidades que deseen suscribir convenios con el Icetex con la finalidad de ampliar, financiar y cubrir los costos educativos de la población que deseen atender.
  - Instituciones de Educación Superior (IES) quienes reciben los desembolsos de los créditos gestionados a través de la Entidad.
  - Los fondos administrados por el Icetex, correspondiente al portafolio de recursos de terceros tanto públicas como privadas, con el fin de ejecutar por cuenta de ellas sus diferentes programas y proyectos de educación para la población objetivo que éstas han determinado atender; fortaleciendo los mecanismos de la cobertura en educación que busca el país.

- **Entes de Control:**
  - Gobiernos, organismos internacionales e instituciones de educación superior del exterior, ya que el Icetex, en virtud de la cooperación internacional, administra las ofertas de becas que hacen al país.
  - Superintendencia Financiera de Colombia, Procuraduría, Contraloría y la Contaduría General de la Nación como entes de control.
  - Superintendencia de Industria y Comercio, regula y controla la adecuada prestación de los servicios y funge de autoridad de protección de datos personales.
  - Ministerio de Hacienda - manejo de presupuesto.
  - Ministerio de Educación al cual se encuentra vinculado el Icetex.
  - Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, controla la adopción por parte de las Entidades del Estado del MSPI de Gobierno Digital.
- **Proveedores:**

  Estas partes interesadas se ven afectadas en algún sentido por el avance y resultados del Modelo de Seguridad y Privacidad Digital, es así como se mantiene una comunicación fluida conforme a su partición e interacción con el modelo y resultados de las acciones tomadas dentro del mismo. El grado de comunicación con estas partes interesadas depende del nivel clasificación de la información y administración del riesgo definido por el Instituto. Los proveedores se distribuyen así:
  - Personas Naturales: prestan servicios de calidad que cumplen con la normativa interna y externa, como parte de las obligaciones contractuales en materia de seguridad digital y así preservar la confidencialidad de la información gestionada.
  - Personas Jurídicas: prestan servicios de calidad que cumplan con la normativa interna y externa, así como las obligaciones contractuales en material de seguridad digital.

  Las expectativas de las partes interesadas son:

PARTES INTERESADAS	NECESIDADES Y EXPECTATIVAS
Funcionarios	• Tener la confianza de que se cumple la reglamentación para la protección de sus datos personales. • Contar con herramientas y capacitación que apoyen la seguridad digital en el desarrollo de sus funciones dentro de la Entidad. • Participar en la gestión del sistema de seguridad digital aplicando adecuadamente las políticas de seguridad digital. • Adecuada implementación de controles de seguridad digital para protección de los activos de información.
Beneficiarios, Becario, participantes de programas:	• Tener la confianza de que se cumple la reglamentación para la protección de sus datos personales, que se cuenta con procesos y plataformas tecnológicas que entreguen información de forma confiable y oportuna de acuerdo con sus requerimientos. • Mantener los niveles de seguridad adecuados en los servicios de información de la plataforma tecnológica de la Entidad.

PARTES INTERESADAS	NECESIDADES Y EXPECTATIVAS
Ciudadanos	• Aportar en el fortalecimiento de la política de protección de datos personales cuando se den cambios de interés a la comunidad. • Participan en programas promovidos por Icetex y aliados estratégicos de la Entidad.
Entes de control Gobiernos, organismos internacionales e instituciones de educación superior del exterior	• Tener la confianza de que la información relacionada con la administración de las becas ofrecidas por ellos se maneje de manera segura y transparente, cumplimiento de los acuerdos internacionales.
Entes de control	• Dar cumplimiento a la legislación en temas relacionados con seguridad digital, protección de datos personales, transparencia y acceso a la información pública, implementación efectiva de los controles de seguridad formulados por los diferentes modelos de control de seguridad: Modelo Integrado de Planeación y Gestión, Modelo de seguridad y privacidad de la información, circulares externas de la Superintendencia Financiera de Colombia.
Contratista Persona Natural	• Tener la confianza de que se cumple la reglamentación para la protección de sus datos personales. • Contar con herramientas y capacitación que apoyen la seguridad digital en el desarrollo de sus funciones dentro de la Entidad. • Participar en la gestión del sistema de seguridad digital aplicando adecuadamente las políticas de seguridad digital. • Desarrollar los compromisos de seguridad digital pactados con la Entidad. • Adecuada implementación de controles de seguridad digital para protección de los activos de información y la adecuada gestión de datos personales.
Proveedores Personas Jurídicas	• Contar con condiciones y ambientes seguros para el desarrollo de sus actividades y garantías del cumplimiento de las políticas y normas sobre seguridad digital. • Desarrollar los compromisos de seguridad digital pactados con la Entidad. • Participar en la gestión del sistema de seguridad digital aplicando adecuadamente las políticas de seguridad digital.
Aliados estratégicos	• Contar con las condiciones de ciberseguridad, seguridad y privacidad adecuadas de gestión de riesgos para el manejo de la información. • Desarrollar los compromisos de seguridad digital pactados con la Entidad.

Tabla 2. *Expectativas de las partes interesadas*

Con el fin de cubrir las expectativas y necesidades del Sistema de Gestión de Seguridad Digital se tiene un inventario de las partes interesadas.

7.1.3. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DIGITAL

El Icetex a través de su Modelo de Seguridad y Privacidad Digital - MSPI, implementa el Sistema de Gestión de Seguridad Digital y asegura el cumplimiento de los requisitos legales atribuibles de acuerdo con la naturaleza de la Entidad, que son indispensables para la prestación de los servicios ofrecidos.

El MSPI está construido teniendo como marco de referencia el estándar internacional NTC-ISO-IEC 27001 y los requerimientos de Gobierno Digital del Ministerio de Tecnologías de la Información y Comunicaciones de Colombia.

El alcance del Sistema de Gestión de Seguridad Digital es proteger la confidencialidad, integridad y disponibilidad de la información institucional, de funcionarios, de contratistas, de beneficiarios, de proveedores y de aliados estratégicos de la Entidad, así como la plataforma tecnológica y sistemas de información en todos los procesos del Icetex a nivel nacional.

7.2. LIDERAZGO

7.2.1. LIDERAZGO Y COMPROMISO

El Icetex cuenta con el Comité de Seguridad de la Información conformado por miembros de la Alta Dirección con el fin de conseguir los objetivos para la implementación del MSPI, participa como el patrocinador del Sistema de Gestión de Seguridad Digital y en consecuencia provee los recursos necesarios para el funcionamiento de este, pero así mismo vela por el control de la operación.

Con el propósito de garantizar el éxito de su implementación, el Comité de Seguridad de la Información cumple con las siguientes funciones:

- Establece, divulga y asegura la adopción de la política general, los objetivos y las políticas específicas de seguridad y privacidad digital y los requisitos del MSPI en los procesos de la Entidad.
- Comunicar en la Entidad la importancia del MSPI.
- Planear y disponer de los recursos necesarios (presupuesto, personal, tiempo etc.) para la adopción del MSPI.
- Revisa que el MSPI consiga los resultados previstos y realiza revisiones periódicas de la adopción del MSPI.

El Comité de Seguridad de la Información está conformado mediante acto administrativo, señalando las funciones, miembros del comité y su funcionamiento.

7.2.2. POLÍTICA DE SEGURIDAD DIGITAL

Los funcionarios, contratistas y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información, adoptan los lineamientos contenidos del Sistema de Gestión de Seguridad Digital y en los documentos relacionados, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

La Política Global de Seguridad Digital establece la base respecto al comportamiento de personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la Entidad,
se encuentra soportada por políticas específicas, los cuales guían el manejo adecuado de la información del Instituto. En complemento, se establecen controles los cuales se fundamentan en los dominios y objetivos de control del Anexo A de la norma NTC-ISO-IEC 27001.

La Oficina de Riesgos revisa y propone actualización de la Política Global y las políticas específicas de seguridad digital, que se hayan documentadas en la Manual de Políticas de Seguridad Digital.

La implementación de cada política en el Instituto se realiza a través de un procedimiento, guía o controles, para garantizar la ejecución de esta, propendiendo para que los objetivos de seguridad se alcancen.

7.2.3. ROLES, RESPONSABILIDADES Y AUTORIDADES DE LA ORGANIZACIÓN

El gobierno de seguridad digital proporciona la dirección estratégica para lograr el cumplimiento el objetivo de seguridad digital, garantizando una adecuada gestión de los riesgos, una asignación y uso apropiado de los recursos y definición de roles y responsabilidades.

El Icetex define la siguiente estructura organizacional de gobierno de seguridad digital para el establecimiento, implementación, sostenimiento, operación, revisión, monitoreo y optimización del MSPI:

***Gráfico 3**: Estructura de Gobierno de Sistema de Gestión Seguridad Digital*

En la siguiente tabla se resumen las responsabilidades pertinentes a la operación del Sistema de Gestión de Seguridad Digital, acorde con el "Manual de Políticas de Seguridad Digital" (M11):

Rol: Junta Directiva

Tema de Responsabilidad	Responsabilidades
Sistema de Gestión de Seguridad Digital	• Revisa y aprueba las Políticas de Seguridad Digital y de Tratamiento de Datos Personales. • Recibe y conoce los resultados del Sistema de Gestión de Seguridad Digital, especialmente en la evaluación referente a la confidencialidad, integridad y disponibilidad de la información, identificación de ciber amenazas, resultados de la evaluación de efectividad de los programas de ciberseguridad, propuestas de mejora en materia de ciberseguridad y resumen de los incidentes de ciberseguridad que afectaron la entidad.

Rol: Comité de Seguridad de la Información

Tema de Responsabilidad	Responsabilidades
Direccionamiento estratégico del Sistema de Gestión de Seguridad Digital. Revisión y apoyo a la gestión de Seguridad Digital	• Actualiza y presenta ante la Junta Directiva la actualización de Políticas de Seguridad Digital y de Protección de Datos Personales. • Realiza revisiones periódicas (trimestrales) de la adopción del MSPI, y según los resultados de esta revisión definir las acciones pertinentes. • Aprueba las metodologías para el análisis de riesgos de seguridad y clasificación de la información. • Analiza los incidentes de seguridad digital que le son escalados y activa el procedimiento de contacto con las autoridades y grupos de interés especial, cuando lo estime necesario. • Analiza y suministra los recursos técnicos y humanos necesarios para gestionar efectivamente el riesgo de seguridad digital y ciberseguridad.

Rol: Jefes de área - Lideres de Proceso

Tema de Responsabilidad	Responsabilidades

Propiedad y mantenimiento del inventario de activos de información	• Cumple con los controles para los activos de información. • Identifica, clasifica y valora los activos de información, (Dominio A.8). • Identifica los activos de información que se entregan a terceros (aliados estratégicos, proveedores). El detalle de las responsabilidades se encuentra en las Políticas de Seguridad Digital, el Procedimiento de identificar y clasificar activos de información, Guía para clasificar de activos de información, Guía para el manejo de los activos de información y etiquetado y Procedimiento de Intercambio de información digital con terceros.
Gestión de riesgos de seguridad digital	• Identifica, analiza, valora los riesgos de seguridad digital • Asegura la ejecución de los controles de seguridad digital • Realiza el tratamiento de riesgos de seguridad digital • Reporta eventos o incidentes de seguridad de la información que evidencies fallas, accesos no autorizados o pérdida de información (A.16.1.2). • Atender los Incidentes presentados. El detalle se encuentra en el procedimiento de gestionar riesgos de seguridad de la información y la Guía de metodología de gestión de riesgos de seguridad y Procedimiento de gestión de riesgos de seguridad de la información.
Plan de continuidad de negocio	• Genera Planes de contingencia con la debida seguridad.
Lista de chequeo	• Diligencia la lista de seguimiento al Sistema de Gestion de seguridad Digital.
Permisos de acceso a la plataforma tecnológica	• Atiende las necesidades de los colaboradores del equipo de trabajo en tema de accesos y desvinculaciones a los sistemas de información y herramientas tecnológicas. El detalle se encuentra en el Procedimiento de asignación y desvinculación de usuarios.

Rol: Supervisores

Tema de Responsabilidad	Responsabilidades
Gestión de Riesgos de proveedores y aliados estratégicos	• Incluye en los contratos y acuerdos estratégicos que se celebren con terceros, las medidas y obligaciones pertinentes para la adopción y el cumplimiento de políticas de seguridad digital y de protección de datos personales. • Verifica periódicamente el cumplimiento de las obligaciones contractuales relacionadas en los contratos referente a seguridad digital y ciberseguridad.

Rol: Dirección de Tecnología

Tema de Responsabilidad	Responsabilidades
Gestión de Infraestructura Crítica	• En apoyo de la Oficina de Riesgos identifica la infraestructura crítica que soporta estos servicios. • Identifica y valora la dependencia de los servicios críticos con respecto a los proveedores de servicio. • Define y hace seguimiento a los acuerdos de niveles de servicio que garanticen la prestación de los servicios del Icetex. • Protege contra la pérdida de datos, mediante el apoyo en la definición de respaldos de la información y sus respectivas pruebas regularmente, junto con TI, (A.12.3).
Políticas y lineamientos	• Gestiona el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad en la plataforma tecnológica. • Define lineamientos que permitan garantizar la confidencialidad, integridad y disponibilidad de la información a través de los diferentes componentes y controles tecnológicos implementados.
Sistemas de información	• Establece los requerimientos mínimos de seguridad que deben cumplir los sistemas de información que se desarrollen, actualicen o adquieran para uso de la entidad. • Desarrolla pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información con el fin de detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.
Plan de Recuperación de Desastres	• Asegura la existencia del plan de recuperación ante desastres para la infraestructura tecnológica y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados, incorporando los controles de seguridad digital y ciberseguridad. • Prueba los planes de recuperación ante desastres y los planes de contingencia ante escenarios de posibles ataques cibernéticos, indisponibilidad y afectación a la integridad y de la confidencialidad.
Gestión de riesgos	• Implementa controles en las plataformas tecnológicas definidos en las normas internas y externas de seguridad digital. • Implementa controles para mitigar los riesgos que pudieran afectar la seguridad de información confidencial, en reposo o en tránsito. • Emplea mecanismos para la adecuada autenticación y segrega las funciones y responsabilidades de los usuarios con privilegios de administrador o que brindan soporte remoto, para mitigar los riesgos de seguridad digital. • Define los perfiles con la debida segregación de funciones en los sistemas de información. • Incorpora dentro del ciclo de vida del desarrollo del software, incluyendo servicios web

	y apps, que procesan la información confidencial de la entidad o de los clientes (desde las etapas iniciales tales como levantamiento de requerimientos hasta las pruebas de seguridad pertinentes y producción), aspectos relativos con la seguridad digital que permitan mitigar dicho riesgo. • Asegura la plataforma tecnológica de acuerdo con los lineamientos de la normativa interna y externa sobre seguridad digital.
Gestión de incidentes	• Correlación de eventos, monitoreo y alertamiento de seguridad digital. • Cumple con las etapas de gestión de incidentes de ciberseguridad.

Rol: Secretaria General

Tema de Responsabilidad	Responsabilidades
Grupo de Talento Humano	• Establece los deberes de seguridad a la selección, vinculación, durante la ejecución, cambio del empleo y terminación del contrato. • Lidera la emisión y cumplimiento de las normas para el Teletrabajo. • Informa sobre terminación o cambios de responsabilidades de los funcionarios, (Anexo A.7.3.1)
Grupo de Transformación y Desarrollo Organizacional	• Define el personal para concientización y capacitación. • Divulga la capacitación. • Hace medición del cumplimiento de la capacitación.
Grupo de Administración de Recursos Físicos	• Define y ejecuta los controles de acceso físico en oficinas e instalaciones. • Diseña y aplica protección contra amenazas externas y ambientales. • Revisa la conveniencia de contar con un seguro que cubra los costos asociados a ataques cibernéticos.
Grupo de Gestión Documental	• Custodia de la información física
Grupos de Contratación y Acuerdos Estratégicos	• Verifica que los contratos o convenios de ingreso que por competencia deban suscribir los sujetos obligados, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso.

Rol: Oficina de Riesgos

Tema de Responsabilidad	Responsabilidades
Gestión de Riesgos	• Apoya a los Lideres de Procesos en la gestión de riesgos de seguridad.
Gestión de incidentes de seguridad digital	• Cumple con las etapas de gestión de incidentes de ciberseguridad. • Reporta los incidentes a Comité de Seguridad de la Información, Junta Directiva y a entes regulatorios de acuerdo con la situación presentada y en cumplimiento a las normativas existentes. • Monitoreo y cierre de incidentes.
Gestión de activos de información	• Apoyo a los Lideres de Proceso en el inventario y clasificación de los activos de información. • Elaboración y divulgación de los documentos de Instrumentos de Gestión.
Capacitación y sensibilización en materia de seguridad digital	• Elabora y ejecuta el Plan de capacitación. • Promueve la cultura de seguridad digital en todos los funcionarios, contratistas y al personal provisto por terceras partes.
Documentación del Sistema de Gestión de Seguridad Digital	• Actualiza las Políticas de Seguridad Digital y de Protección de Datos Personales, con frecuencia anual. • Crea y actualiza la documentación del Sistema de Gestión de Seguridad Digital.
Seguimiento en continuidad	• Verifica en las pruebas de contingencia que se realicen con la debida protección a la información. • Verifica, revisa y evalúa la continuidad de la seguridad de la información.
Reporte a la Junta Directiva y Comité de Seguridad de la Información	• Reporta semestralmente los resultados de la gestión de seguridad digital y ciberseguridad, especialmente en la evaluación referente a la confidencialidad, integridad y disponibilidad de la información, identificación de ciber amenazas. • Asesora a la Alta Gerencia y la Junta Directiva en temas que considere necesarios sobre seguridad digital y ciberseguridad para que estas últimas puedan hacer seguimiento y tomar las decisiones adecuadas en esta materia. • Presenta ante el Comité de Seguridad de la Información el estado del SGSD con frecuencia trimestral, atendiendo los compromisos y observaciones que se presenten en las sesiones.
Cumplimiento normativo de la seguridad digital	• Adopción del marco de referencia de la ISO27001 y el Modelo de Seguridad y Privacidad de la Información de MInTic. • Monitoreo y verificación del cumplimiento de las políticas y procedimientos que se establezcan en materia de seguridad digital y ciberseguridad. • Verifica el cumplimiento de las obligaciones contenidas en la normativa en el tema de seguridad digital. • Implementa un sistema de gestión para la ciberseguridad. • Establece indicadores para medir la eficacia y eficiencia de la gestión de la seguridad digital y la ciberseguridad.

Presupuesto de seguridad digital	• Sugiere los presupuestos de seguridad digital y ciberseguridad. Dichos presupuestos deben manejarse de manera diferenciada a los de operaciones y tecnología de la información. • Revisa y propone los recursos de personal necesario para la gestión de la seguridad digital del Instituto.
Gestión de usuarios	• Controla el acceso a la información, apoyándose con TI, Administrativa, talento humano y contractual (Dominio A.9).
Gestión de datos personales	• Identifica la información que contiene datos personales, teniendo en cuenta la ley 1581 (A.18.1.4).
Gestión de comunicaciones	• Elabora y desarrolla el Plan de sensibilización y comunicación.
Roles y responsabilidades del SGSD	• Define y establece los roles y responsabilidades relacionados con la seguridad digital.

Rol: Oficina Asesora Jurídica

Tema de Responsabilidad	Responsabilidades
Asesoría jurídica aplicable a la Seguridad Digital	• Brinda asesoría a los procesos de la Entidad en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información. • Brinda asesoría al Comité Institucional de Gestión y Desempeño en materia de temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información. • Representa a la Entidad en procesos judiciales ante las autoridades competentes relacionados con seguridad y privacidad de la información. • Apoya y asesora a los procesos en la elaboración del Índice de Información clasificada y reservada de los activos de información de acuerdo con la regulación vigente.

Rol: Usuarios

Tema de Responsabilidad	Responsabilidades
Compromiso con el sistema de gestión de seguridad digital	• Los funcionarios, contratistas, pasantes y personal provisto por terceras partes que realicen labores en o para el Icetex, tienen la responsabilidad de cumplir con las políticas, normas internas y externas, procedimientos y controles referentes a la seguridad digital.

Tabla 3. *Roles y responsabilidades específicos para la seguridad digital.*

7.2.4. OBJETIVO DE SISTEMA DE GESTIÓN DE SEGURIDAD DIGITAL

Para apoyar el cumplimiento del objetivo estratégico del Instituto, que menciona "Optimizar los procesos clave y fortalecer el sistema de administración de riesgo" se adopta el Sistema de Gestión de Seguridad Digital cuyo objetivo es: Implementar, operar y mantener las medidas de control que permitan el tratamiento adecuado de los riesgos seguridad digital, para garantizar la protección de la información de las partes interesadas del Icetex.

Objetivos Específicos

- Gestionar los riesgos de seguridad digital
- Fortalecer la cultura en seguridad digital
- Implementar los controles necesarios para mantener la confidencialidad, integridad y disponibilidad de la información.

Para el desarrollo de este objetivo se cuenta con:

- Recursos: plataforma tecnológica y/o procedimental específica identificada para el tratamiento de la causa, presupuesto para implementación de controles de seguridad, talento humano del Instituto o externo que apoya la gestión de la seguridad digital.
- Roles y responsabilidades definidas.
- Evaluación: mecanismos que van dirigidos a fortalecer y mantener los controles mitigadores del riesgo, a través de autoevaluaciones, indicadores, planes de acción y auditorias.

Para el cumplimiento del objetivo del Sistema de Gestión de Seguridad Digital se dispone de indicadores que en conjunto con las evaluaciones permite iniciar el proceso de mejora continua del Sistema de Gestión de Seguridad Digital, para alcanzar el nivel propuesto. La Oficina de Riesgos es la responsable de realizar el seguimiento al cumplimiento del objetivo.

7.3. PLANIFICACIÓN

7.3.1. IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN E INFRAESTRUCTURA CRÍTICA

Para realizar una adecuada planificación del sistema de gestión de seguridad digital, la Entidad identifica dentro de un inventario los activos de información que son fundamentales para el cumplimiento de sus funciones institucionales. De acuerdo con la normativa NTC-ISO-IEC 27001, al modelo de seguridad y privacidad de información y la normatividad vigente en materia de acceso a la información pública, los activos son claramente identificados, se les asigna un propietario y se realiza una apropiada clasificación de la información de acuerdo con los requisitos legales, valor y criticidad de estos.

El Manual de Políticas de Seguridad Digital contiene las políticas de gestión de activos, donde se definen las normas para el uso apropiado de los activos y la clasificación y manejo de la información.

El inventario y clasificación de activos se elabora de acuerdo con la Guía de gestión y clasificación de activos de información y procedimiento de inventario y clasificación de activos de información.

7.3.2 VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DIGITAL

La metodología de gestión de riesgos de seguridad digital permite identificar, analizar y valorar los riesgos relacionados con la seguridad digital que dificulten el logro de los objetivos propuestos por los procesos, así como determinar el tratamiento y aceptación de los riesgos remanentes. La gestión de riesgos es continua y constituye un ciclo de mejoramiento continuo (Planear-Hacer-Verificar-Actuar) y desarrolla de acuerdo con el Procedimiento Gestionar Riesgos de Seguridad de la Información.

La gestión de riesgos es coordinada por la Oficina de Riesgos y reporta al Comité de Seguridad de la Información los resultados de la gestión, identificación de amenazas, propuestas de mejora y el resumen de los incidentes de seguridad y ciberseguridad. A continuación, se describe el flujo de gestión de riesgos:

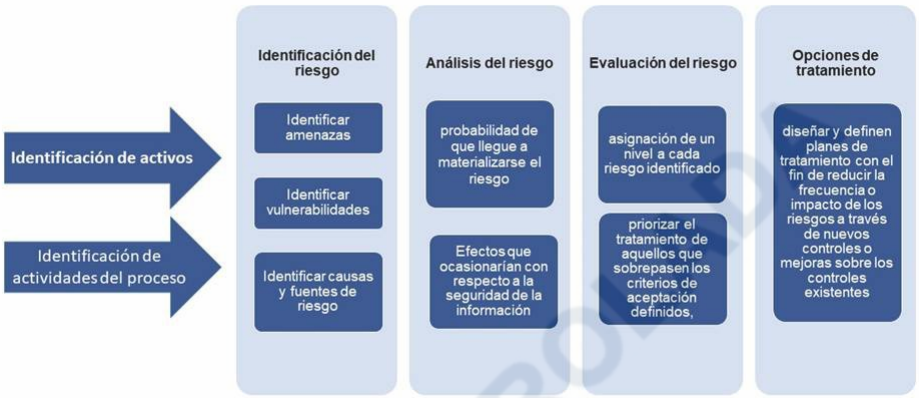

***Gráfico 4**: Proceso de Gestión de Riesgos de Seguridad Digital*

7.3.3. PLAN DE TRATAMIENTO DEL RIESGO

De acuerdo con la metodología establecida para las zonas de riesgo grave y crítico o causas sin controles identificados, se deben diseñar y definir planes de tratamiento, con el fin de reducir la frecuencia o impacto de los riesgos a través de nuevos controles o mejoras sobre los controles existentes, dicho plan de tratamiento se documenta en el Aplicativo de Gestión de Riesgos.

Los planes de tratamiento deben contener las opciones (controles) pertinentes y apropiadas para el tratamiento de riesgos, fechas y responsables con el objetivo de realizar trazabilidad.

Los dueños de los riesgos deben realizar la aprobación formal del plan de tratamiento de riesgos y esta aceptación debe llevarse a la revisión en el Comité de Seguridad de la Información.

El resultado de la selección de controles para el tratamiento de los riesgos de seguridad se documenta en la Declaración de Aplicabilidad, que está conformada por los controles aplicables, basados en el anexo A de la norma técnica colombiana NTC ISO/IEC 27001.

7.4. SOPORTE

El Icetex suministra soporte al Sistema de Gestión de Seguridad Digital, disponiendo de los recursos, competencias, toma de conciencia, comunicación e información documentada, descritas a continuación:

7.4.1. RECURSOS

La Entidad determina y proporciona los recursos necesarios para la adopción, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad Digital:

- Talento humano competente, las competencias y funciones del personal requeridos para apoyar el Sistema de Gestión de Seguridad Digital, que se encuentran descritas en el Manual de Funciones.

  Se garantiza realizar la vinculación de personal adecuado y las actividades que permitan su desarrollo en la Entidad, a través de los procesos de Ingreso, Permanencia y Administración de personal y Contractual.

- Infraestructura física y plataforma tecnológica (software y hardware) y equipos de comunicación, que soportan el desarrollo de las actividades de cada uno de los procesos de la Entidad y apoyan en la preservación de la seguridad digital.

7.4.2. COMPETENCIA, TOMA DE CONCIENCIA Y COMUNICACIÓN

COMPETENCIA

El Icetex busca contar con una correcta comunicación, sensibilización y concientización con respecto a la seguridad y privacidad digital en la que todos sus funcionarios y contratistas estén al tanto de la política de seguridad y privacidad, conozcan su rol en el cumplimiento del MSPI, beneficios y consecuencias de no poner en práctica las reglas definidas en el modelo (desde el punto de vista de seguridad y privacidad de la información).

Para ello propende que los diferentes empleos que conforman la planta de personal del Instituto cuentan con la educación, formación o experiencia necesaria, con respecto a la seguridad digital, para la ejecución de sus funciones. La competencia es dividida en diferentes niveles de acuerdo con el fin particular que tiene cada funcionario dentro del Sistema de Gestión de Seguridad Digital:

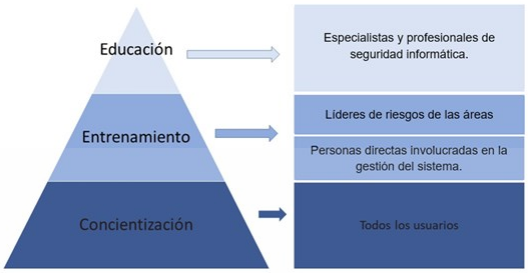

***Gráfico 5**. Niveles de competencia en seguridad digital.*

- Educación: integra todas las habilidades de seguridad y las competencias de las diversas especialidades funcionales, agrega un estudio multidisciplinario de conceptos, problemas y principios (tecnológicos y sociales), y se esfuerza por producir especialistas con competencias técnicas y profesionales capaces de visión y respuesta proactiva.
- Entrenamiento: busca enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo.
- Concientización: tiene como objetivo principal impactar sobre el comportamiento de una población, o reforzar buenas prácticas de seguridad digital, el detalle del plan de concientización se expone en el siguiente numeral.

La gestión para el desarrollo de competencias se detalla en el Plan de Capacitación en Seguridad de la Información.

TOMA DE CONCIENCIA

La concienciación está orientada a la difusión del Sistema de Gestión de Seguridad Digital, a través de la incorporación de un conocimiento en seguridad digital y al mismo tiempo lograr la adopción y asimilación de componentes de este modelo.

Los planes de capacitación del Instituto y sensibilización anuales pueden ser modificados cuando aparezcan nuevos riesgos críticos, nuevas leyes y regulaciones o cuando se materialice un incidente. El Comité de Seguridad de la Información vela porque existan y se dispongan los recursos necesarios para esta actividad.

Como parte de la evaluación de la eficacia de la sensibilización, se ejecuta pruebas de ingeniería social que tiene como finalidad medir el grado de interiorización en aspectos de seguridad digital que han recibido los funcionarios y contratistas. La gestión de concienciación se detalla en el documento Plan de Capacitación en Seguridad Digital.

COMUNICACIÓN

La Oficina de Riesgos identifica las necesidades de comunicaciones internas y externas relacionadas con la seguridad y privacidad de la información, definiendo qué será comunicado, cuándo, a quién, quién debe comunicar y finalmente definir los procesos para lograrlo. El detalle de estas actividades puede ser consultado en el Plan de Sensibilización y Comunicación de Seguridad Digital.

De igual manera, se cuenta con canales para una adecuada comunicación con las organizaciones gubernamentales y demás grupos pertinentes para mantener un intercambio de conocimientos que permita la gestión adecuada de la seguridad digital y la integración ante la ocurrencia de incidentes de ciberseguridad.

7.4.3. INFORMACIÓN DOCUMENTADA

Los documentos generados por el Sistema de Gestión de Seguridad Digital cumplen con lo establecido en el Sistema de Gestión de Calidad en cuanto a:

- Aprobación de los documentos antes de su publicación.
- Revisión y actualización de los documentos cuando se requiera.
- Comprobación periódica de la vigencia de las versiones, de su disponibilidad a los usuarios autorizados, de su almacenamiento, transmisión y destrucción conforme a las tablas de retención documental.
- Verificación de legibilidad e identificación, para prevenir el uso de documentos obsoletos.

La implementación del Sistema de Gestión de Seguridad Digital implica una correcta recopilación de documentos y registros, de acuerdo con la norma NTC-ISO-IEC 27001, las guías del MSPI del MINTIC y la estructura documental del Sistema de Gestión de Calidad del Instituto. El listado de documentos, procedimientos, guías y registros obligatorios se detalla en el anexo 1 Documentación del Sistema de Gestión de Seguridad Digital.

8. OPERACIÓN

Una vez culminada las actividades del MSPI de la fase de 7.3 Planificación, se implementa los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad digital identificados.

8.1. PLANIFICACIÓN E IMPLEMENTACIÓN

La Entidad realiza la planificación e implementación de las acciones determinadas en el plan de tratamiento de riesgos, como resultado se generan los siguientes documentos, que son aprobados en el Comité de Seguridad de la Información

- Plan de implementación de controles de seguridad y privacidad de la información
- Evidencia de la implementación de los controles de seguridad y privacidad de la información

9. EVALUACIÓN DEL DESEMPEÑO DEL MODELO

9.1. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

El propósito del seguimiento, medición, análisis y evaluación es comprobar la efectividad, eficiencia y eficacia de los controles, el tratamiento de riesgos, el plan operacional, la gestión de incidentes y la medición del objetivo de seguridad digital; brindando un soporte para el sostenimiento y optimización del Sistema de Gestión de Seguridad Digital.

Para el desarrollo del seguimiento y medición se establece el Plan de seguimiento y evaluación del SGSD, el cual es aprobado por el Comité de seguridad de la Información.

Para realizar una medición adecuada el Instituto ha establecido formalmente los siguientes indicadores, el seguimiento es realizado por parte de la Oficina Asesora de Planeación:

OBJETIVOS DEL MODELO	INDICADORES
Gestionar los riesgos de seguridad de la información.	I.1 - Gestión de riesgos (Indicador operativo) 1.2 Gestión de activos de información (Indicador operativo)
Fortalecer la cultura en seguridad de la información.	I.3 - Concienciación en seguridad digital (Indicador operativo)
Implementar los controles necesarios para mantener la confidencialidad, integridad y disponibilidad de la información.	I.4 – Cumplimiento normativo (Indicador operativo)

Tabla 4. *Alineación de objetivos de MSPI e indicadores*

9.2. AUDITORIA INTERNA

La auditoría interna al Sistema de Gestión de Seguridad Digital de acuerdo con la norma ISO27001 y al MSPI juega un papel importante en la vigilancia del cumplimiento de las políticas y procedimientos establecidos por la Oficina de Riesgo en cuanto a seguridad digital y por los controles establecidos por los dueños de la información para la mitigación de riesgos.

Para ello, la Oficina de Control Interno, de forma autónoma puede auditar cualquiera de los componentes y el correcto funcionamiento de los siguientes aspectos:

- Cumplimiento en la implementación del Sistema de Gestión de Seguridad Digital.
- Cumplimiento normativo de acuerdo con los tiempos establecidos por Ley.
- Cumplimiento en identificación y clasificación de los activos de información.
- Cumplimiento en implementación de controles para protección de la información dada su clasificación.
- Cumplimiento en identificación y análisis de riesgos.
- Cumplimiento en implantación de planes de tratamiento.
- Cumplimiento en la ejecución de los planes de sensibilización y capacitación.

La auditoría se realiza de forma independiente, los hallazgos encontrados se tratan conforme al procedimiento acciones correctivas, preventivas y de mejora.

9.3. REVISIÓN POR LA DIRECCIÓN

En el Comité de Seguridad de la Información se evalúa el Sistema de Gestión de Seguridad Digital del Icetex y determina las mejoras que se deben realizar al mismo. En la revisión por parte de la Junta Directiva y la Alta Dirección se verifican los siguientes aspectos:

- Estado de las acciones de revisiones anteriores.
- Cambios de las cuestiones internas y externas que sean pertinentes al Sistema de Gestión de Seguridad Digital.
- Retroalimentación sobre el desempeño del Sistema de Gestión de Seguridad Digital incluyendo no conformidades, acciones correctivas, seguimiento y resultados de las mediciones.
- Resultados de auditorías.
- Cumplimiento de los objetivos del Sistema de Gestión de Seguridad Digital.
- Resultados de la evaluación de riesgos y estado del plan de tratamiento de riesgos.
- Oportunidades de mejora continua.

Los elementos de salida de la revisión por la Dirección incluyen las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el Sistema de Gestión de Seguridad Digital.

10. MEJORAMIENTO CONTINUO

El Icetex en la mejora del Sistema de Gestión de Seguridad Digital considera las no conformidades, acciones correctivas y mejora continua.

10.1. NO CONFORMIDADES Y ACCIONES CORRECTIVAS

El Icetex cuenta con un procedimiento y metodología que se adapta al Sistema de Gestión de Seguridad Digital, permitiendo llevar a cabo las acciones para determinar, prevenir y eliminar las causas de No conformidades y Oportunidades de mejora se presenten en los componentes del sistema auditado, las cuales se pueden observar en el Procedimiento "Acciones correctivas y de mejora" (E1-2-10). Las no conformidades pueden tener origen en fuentes como:

- Incidentes relacionados con la seguridad y privacidad digital.
- Informes de auditorías.

- Gestión del riesgo y planes de tratamiento de riesgos de seguridad digital.
- Revisión por la dirección.

10.2. MEJORA CONTINUA

La Entidad adopta la mejora continua para garantizar la eficacia del Sistema de Gestión de Seguridad Digital a través del uso de la Política de Seguridad Digital, de los Objetivos de este sistema, de los resultados de auditorías, del análisis de eventos de seguridad digital, acciones correctivas y preventivas y la revisión por la dirección.

El mejoramiento continuo PHVA (Planear, Hacer, Verificar, Actuar) es una estrategia efectiva de la Entidad para la implementación, sostenimiento y optimización del Sistema de Gestión de Seguridad Digital. En seguridad digital el mejoramiento continuo es la revaluación de las medidas de prevención, corrección y evaluación, con el propósito de identificar desviaciones, debilidades y resolver problemas relacionados con el ciclo de mejoramiento continuo y parte de:

- Revisiones del Sistema de Gestión de Seguridad Digital.
- Mediciones de la Eficacia de los Controles.
- Revisiones del Riesgo Residual.
- Realización de Auditorías Internas del Sistema de Gestión de Seguridad Digital.
- Revisión del plan de acción.
- Registro Acciones y Eventos.

11. DOCUMENTOS RELACIONADOS

NOMBRE DEL DOCUMENTO	CÓDIGO
Manual de Políticas de Seguridad Digital	M11
Declaración de Aplicabilidad	F388
Guía Metodológica de gestión de riesgos de seguridad digital	G175
Planes de Capacitación, sensibilización y comunicación en Seguridad Digital	
Identificar y clasificar activos de información	E2-1-13
Indicadores de Gestión del MSPI	
Acciones correctivas y de mejora	E1-2-10

12. ANEXOS

Anexo 1 - DOCUMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DIGITAL

a. DOCUMENTOS REQUERIDOS MSPI

Son los documentos principales y necesarios para cumplir con la norma NTC-ISO-IEC 27001 (se debe tener en cuenta que los documentos del anexo A son obligatorios siempre y cuando el control respectivo sea aplicable)

Documentación obligatoria	Referencia NTC-ISO-IEC 27001	Descripción	Ubicación
El alcance del Sistema de Gestión de Seguridad Digital	cláusula 4.3	La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad digital para establecer su alcance, considerando las cuestiones internas y externas de la organización, y los requerimientos en seguridad digital, de las partes interesadas.	MSPI numeral 4.4 del Modelo de Seguridad y Privacidad Digital.
Política de seguridad digital	cláusulas 5.2	Se debe establecer una política de la seguridad digital adecuada al propósito de la organización.	Manual de Políticas de Seguridad Digital.
El proceso de evaluación de riesgos.	cláusula 6.1.2	La organización, debe definir un proceso de evaluación de riesgos, que permita identificar los dueños de los riesgos, evaluar las consecuencias potenciales, la probabilidad de ocurrencia, los niveles de riesgo, y el valor tolerable de riesgo para la organización.	Procedimiento Gestionar Riesgos de Seguridad de la Información.
Declaración de aplicabilidad	cláusula 6.1.3	Se debe generar una declaración de aplicabilidad, con la justificación de la inclusión o exclusión de los controles presentes en el Anexo A de la norma NTC-ISO-IEC 27001.	Declaración de Aplicabilidad
El proceso de tratamiento de riesgos.	Cláusula 6.1.3	La organización debe mantener documentación del proceso de tratamiento de riesgos, aprobado por los dueños de los riesgos y la aceptación de los riesgos residuales.	Procedimiento Gestionar Riesgos de Seguridad de la Información.
Objetivos del sistema de gestión de seguridad de la digital	Clausula 6.2	La organización debe establecer objetivos coherentes con la política de seguridad, que sean medibles, y tengan en cuenta los resultados de la evaluación de riesgos.	Numeral 6.2 del Modelo de Seguridad y Privacidad Digital
Información documentada de la ejecución de los procesos tratamiento de riesgos y logro de los objetivos de seguridad	Cláusula 8.1	La organización debe planificar, e implementar los procesos para cumplir los requisitos e implementar las acciones determinadas para el tratamiento de riesgos, y lograr los objetivos de la seguridad digital.	Estrategia de Planificación y Control Operacional
Informe sobre los resultados de la evaluación de riesgos	cláusula 8.2	Se debe mantener la información documentada, con respecto a los resultados de la evaluación de riesgos, efectuada según los criterios definidos por la organización.	Matriz de Riesgos de Seguridad Digital
Informe sobre los resultados del tratamiento de riesgos	Cláusula 8.3	La organización debe implementar el plan de tratamiento de riesgos, y mantener la información documentada para los resultados de este proceso.	Procedimiento Gestionar Riesgos de Seguridad de la Información
Inventario de activos	Control A.8.1.1	Se deben identificar los activos asociados con la información e instalaciones de procesamiento de información y se debe elaborar y mantener un inventario de estos activos	Identificar y Clasificar de Activos de Información

Documentación obligatoria	Referencia NTC-ISO-IEC 27001	Descripción	Ubicación
Uso aceptable de los activos	Control A.8.1.3	Se deben identificar reglas para el uso aceptable de activos de información.	Guía para el Manejo de los Activos de Información y Etiquetado
Política de control de acceso	Control A.9.1.1	Se debe documentar una política de control de acceso con base en los requisitos del negocio y de la seguridad digital.	Manual de Políticas de Seguridad Digital
Procedimientos de operación para gestión de TI	Control A.12.1.1	Se deben documentar los procedimientos operativos, o de actividades de sistemas asociados a los recursos de tratamiento y comunicación de la información; tales como procedimientos de apagado de equipos, copias de respaldo, mantenimiento de equipos, entre otros.	Proceso de Gestión de Servicios Tecnológicos
Requisitos para los acuerdos de confidencialidad o no divulgación	Control A.13.2.4	Se deben documentar los requisitos para los acuerdos de confidencialidad, de acuerdo con las necesidades de la organización, para la protección de la información.	Formato de Acuerdo de Confidencialidad
Principios de sistemas seguros	Control A.14.2.5	Se deben documentar y mantener principios para la organización de sistemas seguros.	Procedimiento de Gestión de Requerimientos de Desarrollo Tecnológico
Política de seguridad para proveedores	Control A.15.1.1	Se debe documentar una política de seguridad que establezca los requisitos de seguridad digital para mitigar los riesgos asociados con el acceso de proveedores.	Manual de Políticas de Seguridad Digital
Procedimiento para gestión de incidentes	Control A.16.1.5	Se debe documentar un procedimiento para dar respuesta a los incidentes de seguridad digital	Procedimiento para Reportar y Gestionar Incidentes de Seguridad de la Información
Procedimientos de Continuidad de negocio	Control A.17.1.2	Se debe documentar los procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad digital durante situaciones adversas.	Plan de Recuperación de Desastres
Requerimientos legales, regulatorios y contractuales, y enfoque para cumplirlo	Control A.18.1.1	Se deben mantener documentados los requisitos reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos.	Autodiagnóstico legal de seguridad digital.

b. PROCEDIMIENTOS DEL MSPI

Son aquellos documentos de nivel operativo que indican y aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad digital. Para la implementación del Modelo de Seguridad y Privacidad Digital, la norma NTC-ISO-IEC 27001 establece la documentación e implementación de al menos los siguientes procedimientos:

Procedimiento	Referencia NTC-ISO-IEC 27001	Ubicación
Procedimiento de contacto con autoridades	A.6.1.3	Procedimiento para Reportar y Gestionar Incidentes de Seguridad de la Información
Procedimiento para el etiquetado de la información	A.8.2.2	Manejo y Etiquetado de Activos de Información
Procedimiento para el manejo de activos	A.8.2.3	Manejo y Etiquetado de Activos de Información
Procedimiento para la gestión de medios de soporte removibles	A.8.3.1	
Procedimiento para la disposición de los medios	A.8.3.2	
Procedimiento de registro y retiro de usuarios	A.9.2.1	Procedimiento de Gestión de Accesos y Retiro de Servicios
Procedimiento para la gestión de información secreta de autenticación	A.9.2.4	
Procedimiento para inicio seguro de sesión	A.9.4.2	
Procedimiento para trabajo en áreas seguras	A.11.1.5	
Procedimiento para copias de respaldo	A.12.3	
Procedimiento para controlar la instalación de software en sistemas operativos	A.12.5.1	

Procedimiento de transferencia de información	A.13.2.1	Procedimiento de Intercambio de Información con Terceros Procedimiento de Transferencia Segura de Información
Procedimiento de control de cambios en sistemas	A.14.2.2	Procedimiento de Control de Cambios y Despliegues
Procedimiento de gestión de cambios	A.15.2.2	Procedimiento de Control de Cambios y Despliegues
Procedimiento de gestión de incidentes de seguridad digital	A.16.1.1	Gestionar Incidentes de Seguridad de la Información
Procedimiento para la recolección de evidencia.	A.16.1.7	Guía para el Manejo de Posible Delito Informático
Procedimiento para la protección de propiedad intelectual	A.18.1.2	No se cuenta con el procedimiento

Procedimientos requeridos por la norma NTC-ISO\IEC 27001

La guía número 3 del Modelo de seguridad y privacidad de la información del MINTIC, recomienda la implementación de 22 procedimientos de seguridad de la información, sin embargo, varios de estos coinciden con los requeridos por la norma NTC-ISO-IEC 27001. Los procedimientos adicionales se muestran a continuación:

Procedimiento	Referencia	Ubicación
Procedimiento de capacitación y sensibilización del personal.	Numeral 6.1 Guía 3 del MINTIC	Procedimiento de Gestionar Capacitaciones Institucionales
Procedimiento de ingreso y desvinculación del personal.	Numeral 6.1 Guía 3 del MINTIC	Procedimiento Ingreso Procedimiento de Retiro de Personal
Procedimiento de controles y llaves criptográficas.	Numeral 6.4 Guía 3 del MINTIC	Procedimiento de Transferencia Segura de la Información
Procedimiento de control de acceso físico.	Numeral 6.5 Guía 3 del MINTIC	No se cuenta el procedimiento
Procedimiento de protección de activos.	Numeral 6.5 Guía 3 del MINTIC	Guía de Manejo de Activos y Etiquetado
Procedimiento de retiro de activos.	Numeral 6.5 Guía 3 del MINTIC	No se cuenta con el procedimiento
Procedimiento de mantenimiento de equipos.	Numeral 6.5 Guía 3 del MINTIC	
Procedimiento de gestión de capacidad.	Numeral 6.6 Guía 3 del MINTIC	Procedimiento de Retiro de Personal
Procedimiento de separación de ambientes.	Numeral 6.6 Guía 3 del MINTIC	Procedimiento de Retiro de Personal
Procedimiento de protección contra códigos maliciosos.	Numeral 6.6 Guía 3 del MINTIC	Procedimiento de Retiro de Personal
Procedimiento de aseguramiento de servicios en la red.	Numeral 6.7 Guía 3 del MINTIC	Procedimiento de Retiro de Personal
Procedimiento adquisición, desarrollo y mantenimiento de software.	Numeral 6.9 Guía 3 del MINTIC	Procedimiento de Requerimientos de Desarrollo Tecnológico

Procedimientos adicionales recomendados por el MSPI del MINTIC

c. INSTRUCTIVOS

Este tipo de documentos describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad digital y aunque de acuerdo con la norma NTC-ISO-IEC 27001 y a las guías de implementación de MSPI del MINTIC, no son obligatorios, es importante considerar y elaborar los instructivos necesarios para que el MSPI sea plenamente eficaz.

d. REGISTROS

Este tipo de documentos proporcionan la evidencia objetiva del cumplimiento de los requerimientos del MSPI. De acuerdo con lo establecido por la norma NTC-ISO-IEC 27001 se deben mantener obligatoriamente los registros que se muestran en la siguiente tabla:

Registro Obligatorio	Referencia NTC-ISO-IEC 27001	Descripción	Ubicación
Registros de formación, habilidades, experiencia y calificaciones	Cláusula 7.2	La organización debe conservar la información documentada apropiada, como evidencia de la competencia.	Hoja de vida de personas
Evidencia sobre los resultados del monitoreo y de la medición	Cláusula 9.1	La organización debe conservar información documentada apropiada como evidencia de los resultados del monitoreo y de la medición.	Indicadores
Evidencia de implementación del programa de auditoría y de los resultados	Cláusula 9.2	La organización debe conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de esta.	Programa de auditoria
Evidencia de los resultados de las revisiones por la dirección	Cláusula 9.3	La organización debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección.	Informe de auditoría (F180) Acta de Comité de Seguridad de la Información (final de año).
Evidencia de no conformidades y resultados de acciones correctivas.	Cláusula 10.1	La organización debe conservar información documentada adecuada, como evidencia de: • la naturaleza de las no conformidades y cualquier acción posterior tomada; y • los resultados de cualquier acción correctiva.	Informe de auditoría (F180)

Registro Obligatorio	Referencia NTC-ISO-IEC 27001	Descripción	Ubicación
Registros de las actividades de usuario, excepciones y eventos de seguridad	Controles A.12.4.1 y A.12.4.3	La organización debe generar evidencia sobre: • los registros de eventos acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información. • Las actividades del administrador y del operador del Sistema.	Formato de Incidentes de seguridad

Registros obligatorios requeridos por la norma NTC-ISO-IEC 27001

e. Guías del MSPI – MinTic

Son guías de mejores prácticas para implementación del MSPI propuestas por el MinTic

	Cláusulas NTC-ISO-IEC 27001						
Guías MSPI	Contexto de la organización	Liderazgo	Planificación	Soporte	Operación	Evaluación y desempeño	Mejora
Guía 1 – Metodología de pruebas de efectividad.						■	
Guía 2 – Política general MSPI.		■					
Guía 3 – Procedimientos de seguridad de la información.					■		
Guía 4 – Roles y responsabilidades.		■					
Guía 5 – Gestión y 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 del negocio.					■		
Guía 11 – Análisis de impacto al negocio.					■		
Guía 12 – Seguridad en la nube.					■		
Guía 13 – Evidencia digital.					■		
Guía 14 – Plan de comunicación, sensibilización y capacitación.			■				
Guía 15 – Auditoria.						■	
Guía 16 –Evaluación del 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.					■		

Alineación Guías MSPI y cláusulas NTC-ISO-IEC 27001

Anexos:
M16 Modelo de seguridad y privacidad digital V5.pdf
Editado por Lina Marcela Carmona Parra, mar 13 2023 08:11 a.m.

Modificaciones

Descripción de cambios

1. Cambio de nombre de Modelo de seguridad y privacidad de la información por Modelo de seguridad y privacidad digital
2. Se realizan ajustes a la introducción
3. Se modifica el orden del contenido
4. Se incluye el apartado Propósitos, Marco jurídico, diagnostico, Composición del MSPI, Planificación, alcance del sistema de gestión de seguridad digital, Valoración de los riesgos de seguridad digital, Identificación de activos de información e infraestructura critica .
5. En las partes interesadas se incluyen los beneficiarios, ciudadanos.
6. Se elimina el apartado de 4.3. Modelo de seguridad y privacidad digital.
7. Se ajustan los roles y las tablas.
8. Se incluyen como anexos Documentación del modelo de seguridad y privacidad digital, documentos requeridos MSPI, Procedimiento del MSPI, Instructivos, Registros, Guías del MSPI

Historial de Versiones

Fecha Vigencia (Acto Adtvo)	Versión	Descripción de Cambios
2022-06-21	5	1. Cambio de nombre de Modelo de seguridad y privacidad de la información por Modelo de seguridad y privacidad digital 2. Se realizan ajustes a la introducción 3. Se modifica el orden del contenido 4. Se incluye el apartado Propósitos, Marco jurídico, diagnostico, Composición del MSPI, Planificación, alcance del sistema de gestión de seguridad digital, Valoración de los riesgos de seguridad digital, Identificación de activos de información e infraestructura critica . 5. En las partes interesadas se incluyen los beneficiarios, ciudadanos. 6. Se elimina el apartado de 4.3. Modelo de seguridad y privacidad digital. 7. Se ajustan los roles y las tablas. 8. Se incluyen como anexos Documentación del modelo de seguridad y privacidad digital, documentos requeridos MSPI, Procedimiento del MSPI, Instructivos, Registros, Guías del MSPI
2021-04-22	4	• Se adiciona el Decreto Nacional 2573 de 214, Decreto 25 de agosto de 2017 y Decreto 620 de 2020. • Igualmente de adicionan los documentos COMPES 3701 Y COMPES 3995 • Lac actualizaciones se aprobaron en los Comités de Desarrollo de fechas junio y diciembre de 2020
2020-4-16	3	Se actualizó el numeral 2 de normativa Se incluyeron los objetivos especificos en el numeral 6.2 Se incluyeron los indicadores en el numeral 9.1 Se amplió el concepto de proveedores en el numeral 4.2 y se complementó el alcance de Sistema de gestión de seguridad digital en el numeral 4.4
2019-3-11	2	Se modifica el alcance del SGSD, se modifica la gestión de riesgos y los objetivos del SGSD, competencias, documentación, plan de continuidad, incidentes, nube, identificación de activos en la parte de identificación de amenazas.
2017-9-20	1	-

¿Ha revisado el documento en su totalidad?
SI