INSTITUTO NACIONAL DE FORMACIÓN TÉCNICA PROFESIONAL

INFOTEP Archipiélago

POLÍTICA DE SEGURIDAD DIGITAL

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia | Nit: 892400461-5 | Teléfonos: (57. 8) 5121350 - 51266 07 | Fax: 512 57 70 | Email: info@infotepsai.edu.co | www.infotepsai.edu.co |
Vigilada MinEducación

1. INTRODUCCIÓN:

El uso masivo de las tecnologías de la información y el incremento en los servicios disponibles en línea, evidencia un aumento significativo en la participación digital de los ciudadanos. Tal aprovechamiento de servicios digitales por parte de los ciudadanos trae nuevas y más sofisticadas formas para atentar contra la seguridad de los sistemas de información del INFOTEP. Por lo tanto la política de seguridad digital busca fortalecer la infraestructura tecnológica de la institución y las capacidades de todo el personal del INFOTEP para identificar, gestionar, tratar y mitigar los riesgos de seguridad en sus actividades dentro de un entorno digital, con el fin de mitigar los riesgos de seguridad de la información.

En los últimos 8 años el concepto de seguridad se ha modificado dos veces, pasando de 'ciberseguridad' a lo que actualmente se conoce como 'seguridad digital', la cual tiene un enfoque más humanístico y es definida como "el conjunto de estrategias para generar confianza en el mundo digital".

El INFOTEP identifica la información como un componente indispensable para lograr los objetivos definidos en la estrategia de la institución, por tal motivo establece un modelo que asegura que la información es protegida de manera adecuada. Es primordial para el INFOTEP ofrecer a sus funcionarios y a toda la comunidad estudiantil un entorno digital abierto, seguro y confiable. Para lograr este objetivo tiene un enfoque de gestión del riesgo que involucra a todos las partes interesadas, mitigando así al máximo la materialización de las amenazas digitales a las cuales estamos expuestos en la actualidad.

El presente documento está organizado de la siguiente manera, siendo esta sección la introducción. La segunda sección presenta los antecedentes y justificación. La tercera presenta a los responsables de liderar la implementación de la política, la cuarta sección los recursos; mientras que la quinta da la definiciones para la comprensión del documento, la sección sexta explica el marco jurídico, la séptima sección define la Política de seguridad digital, presentando su objetivo general, los

objetivos específicos y las estrategias que se implementarán para alcanzarlos, la novena sección muestra los riesgos. Finalmente, en la décima sección se presenta el plan y cronograma de implementación de la política.

2. ANTECEDENTES Y JUSTIFICACIÓN

El uso de las TIC para el desarrollo de las actividades socioeconómicas ha marcado la dinámica de la economía en los países en los últimos años. El INFOTEP con sus funcionarios y comunidad estudiantil no ha sido ajeno al uso de las tecnologías de la información y las comunicaciones con lo cual ha logrado que sus funcionarios y estudiantes tengan mayor acceso a la información haciéndolos más productivos y competitivos.

Por otra parte la adopción de estas tecnologías por parte del INFOTEP y la comunidad en general nos expone a riesgos, amenazas y vulnerabilidades que son aprovechadas por algunas personas para llevar a cabo ataques cibernéticos que pueden afectar de manera negativa a personas e instituciones. Por tal motivo para enfrentar estos riesgos el INFOTEP estableció los lineamientos de Política de Seguridad Digital.

3. RESPONSABLE:

El responsable de liderar la implantación de esta política es el proceso de gestión tecnológica y comunicaciones con el apoyo de la persona encargada de la seguridad y privacidad de la información.

4. RECURSOS

Esta política cuenta con un presupuesto para cada vigencia, donde se define el recurso humano requerido, los servicios contratados y los equipos y/o herramientas que se deben adquirir para la implementación de la política y se puede visualizar en el Plan de Inversión en el proyecto fortalecimiento administrativo y académico, en el presupuesto anual aprobado y en el Plan Anual

de adquisiciones para cada vigencia publicadas en el portal web institucional www.infotepsai.edu.co

5. DEFINICIONES:

Para efectos de la comprensión la política de seguridad de digital del Instituto Nacional de Formación Técnica Profesional, se establecen los siguientes significados de las palabras empleadas en el texto:

Riesgo: es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas.

Riesgo de seguridad digital: es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan.

Gestión de riesgos de seguridad digital: es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.

6. MARCO JURIDICO:

Ítem	Marco	Descripción
1	Decreto 1008 del 14 de Junio de 2018	cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
2	Constitución Política de Colombia	Artículos 11, 12, 13, 14, 17, 21, 22, 24, 29, 44, entre otros. Por ejemplo, Art. 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
3	Ley 527 de 1999 (Comercio Electrónico)	Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
4	Ley 1581 de 2012 (Habeas Data)	Por la cual se dictan disposiciones generales para la protección de datos. Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo a los datos financieros se les continúa aplicando la Ley 1266 de 2008, excepto los principios.
5	Ley 1712 de 2012 (Uso de las TIC)	Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantías del derecho y las excepciones a la publicidad de la información.
6	Decreto 2573 de 2014 (Gobierno en Línea)	Por el cual se establecen los lineamientos generales de la estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones

7. POLÍTICA:

Con base en la Política Nacional de Seguridad Digital CONPES 3854 Se crea esta Política con el fin de abordar las incertidumbres, los riesgos, las amenazas, las vulnerabilidades y los incidentes digitales que se puedan presentar en el INFOTEP. Su objetivo es fortalecer las capacidades de la institución para enfrentar las amenazas que atenten contra la seguridad de la información de la institución. Con el fin de crear un entorno seguro y confiable en el ciberespacio para todos los funcionarios y la comunidad académica del INFOTEP.

Para la implantación de la Política de Seguridad Digital, se ha tomado el foco dado al documento CONPES 3854 donde su principal componente es la gestión de riesgos de seguridad digital, para lo cual el Ministerio de Tecnologías cuenta con una guía metodológica para su correcta implementación en las entidades públicas.

Para el cumplimiento de la Política los lineamientos se establecen o entienden como la directriz o disposición que debe ser implementada por las entidades públicas para el desarrollo de la política y se desarrollan a través de estándares, guías, recomendaciones o buenas prácticas. Así mismo, se entiende por estándar, el conjunto de características y requisitos que se toman como referencia o modelo y son de uso repetitivo y uniforme. Un estándar se construye a través de consenso y refleja la experiencia y las mejores prácticas en un área en particular, implican uniformidad y normalización y son de obligatorio cumplimiento.

La Política de Seguridad Digital se alinea con el Plan Estratégico Institucional y a la Política de Gobierno Digital y de esta se desprenden Políticas como la Política de Seguridad y Privacidad de la Información para dar cumplimiento al Decreto 1008 de 2018.

7.1 OBJETIVO:

Fortalecer la infraestructura tecnológica de la institución y fortalecer las capacidades de todo el personal del INFOTEP para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades dentro de un entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de mitigar los riesgos de seguridad de la información para que la entidad pueda ofrecer así un entorno digital confiable y seguro.

7.2. OBJETIVOS ESPECIFICOS:

- Implementar en el INFOTEP un modelo de gestión de riesgo de seguridad digital.
- Establecer mecanismos de participación de las partes interesadas en la gestión del riesgo de seguridad digital.
- Generar confianza y fortalecer al personal para el uso seguro de entornos digital.
- Generar una estrategia para la protección de la infraestructura del INFOTEP.
  Medir la política desarrollando acciones encaminadas a generar los seguimientos y evaluaciones.

7.3. EJES TEMÁTICOS O LÍNEAS DE ACCIÓN ESTRATÉGICAS:

Los ejes temáticos de esta política son todos los lineamientos que el INFOTEP debe tener implementados para lograr ofrecer a sus funcionarios y a toda la comunidad académica un entorno digital protegido de las amenazas cibernéticas.

- **Modelo de gestión de Riesgo de Seguridad Digital**: para dar cumplimiento a la normatividad de la Política de Seguridad Digital se implementará en el INFOTEP el Modelo de Gestión de Riesgos de seguridad dado por el MINTIC para entidades públicas.

- **Establecer mecanismos de participación de las partes interesadas en la gestión del riesgo de seguridad digital**. se definirán los roles, las responsabilidades y las funciones de las partes interesadas con el fin de involucrar a todos los funcionarios en la construcción y gestión del riesgo en la institución.

- **Generar confianza y fortalecer al personal para el uso seguro de entornos digital.** Concientización y sensibilización para todos los funcionarios por medio de actividades donde se muestre como hacer uso del entorno digital de manera segura.

- **Generar una estrategia para la protección de la infraestructura del INFOTEP**. Implementar la guía de identificación de infraestructura crítica del MINTIC.

- **Fortalecer el mecanismo de identificación, prevención y gestión de incidentes digitales**. En el caso de un incidente de seguridad la entidad debería contar con un procedimiento de gestión de incidentes con el cual puede registrar, monitorear, solucionar e informar a entidades que pueden ayudar a dar solución al mismo.

7.4. METODOLOGÍA PARA IMPLEMENTACIÓN DE LA POLÍTICA:

El INFOTEP cuenta con un plan para la implantación, monitoreo y evaluación de la Política de Seguridad Digital (Modelo de Gestión de Riesgos de Seguridad Digital) donde se describen las actividades que se deben realizar y se identifica al responsable de cada una de fases.

8. RIESGOS

La no implementación de la política de Seguridad Digital puede conllevar a que la entidad no logre sus objetivos, sea ineficiente en sus procesos, que sus tiempos de respuesta a las solicitudes de la ciudadanía no sean los adecuados, lo cual no genera credibilidad hacia la entidad por parte de la ciudadanía.

Para mitigar este riesgo es necesario que todos los funcionarios de la entidad puedan entender la importancia de la política de seguridad digital, debido a que es un compromiso y responsabilidad de todos velar por la seguridad de los activos de información de la institución y se requiere retroalimentación constante, mejoramiento continuo para

rediseñar los instrumentos, herramientas y estrategias que mejoren el fortalecimiento organizacional y garanticen la simplificación de procesos, con un enfoque pedagógico y preventivo.

Para ver en detalle el análisis de riesgos, su valoración y controles dirigirse a la página web de la entidad www.infotepsai.edu.co

9. PLAN DE TRABAJO Y CRONOGRAMA:

El INFOTEP cuenta con un plan y cronograma donde se detallan cada una de las actividades a realizar para la implantación de la política de seguridad digital en la institución.

10. DOCUMENTO DE APROBACIÓN

Acuerdo No. 014 del 23 de mayo de 2019