POLÍTICA DE SEGURIDAD DIGITAL

Institución Universitaria de Envigado
20 de octubre de 2020

Contenido

1. INTRODUCCIÓN

La política de seguridad digital hace parte de la tercera dimensión de MIPG: Gestión con valores para resultados. Esta dimensión tiene el propósito de permitirle a la institución realizar las actividades que la conduzcan a lograr los resultados propuestos y a materializar las decisiones plasmadas en la planeación institucional, en el marco de los valores del servicio público; para concretar las decisiones tomadas en el direccionamiento institucional, y teniendo en cuenta el talento humano del que se dispone, en esta dimensión se abordan los aspectos más importantes que debe atender la institución para cumplir con sus funciones y competencias.

La dimensión de gestión con valores cuenta con dos perspectivas: la primera asociada a los aspectos relevantes para una adecuada operación de la institución “de la ventanilla hacia adentro”; y la segunda, referente a la relación Estado Ciudadano “de la ventanilla hacia afuera”. La política de seguridad digital se encuentra en ambas perspectivas.

La política de seguridad digital busca fortalecer las capacidades de la institución para identificar, gestionar y mitigar los riesgos de seguridad digital en las actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia que permita gestionar la confidencialidad, integridad y disponibilidad como pilares de la seguridad de la información..

2. MARCO CONCEPTUAL

La seguridad digital se entiende como un habilitador de la gestión de la información por el cual las entidades públicas incorporan la gestión de seguridad de la información en todos los procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, y disponibilidad de la datos, así como la protección de los registros personales que tratan las entidades públicas en cumplimiento de la normatividad de protección de datos personales.

Para la comprensión de la política resultan claves los conceptos de activos de información y análisis de riesgo. El primero, en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (información, software, hardware, etc.) que tenga valor para la organización (adaptado a partir de ISO/IEC 27000); respecto al análisis de riesgos, consiste en el proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. El análisis de riesgos proporciona la base para las decisiones sobre el tratamiento de los mismos (adaptado a partir de ISO 31000).

La política de seguridad digital contempla tres pilares fundamentales de la valoración del nivel de riesgo de los activos de información: confidencialidad, integridad y disponibilidad y una serie de acciones de control que son divididas en diferentes dominios en la norma de referencia (ISO 27000)

3. POLÍTICA.

La Institución Universitaria de Envigado establece una política de Seguridad Digital que permita gestionar la confidencialidad, integridad, y disponibilidad de la información en los procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información mediante la aplicación de un proceso estructurado de administración de riesgo, creando un entorno de confianza digital en los grupos de valor y grupos de interés en su interacción con la Institución.

La implementación de esta política se concreta en la adopción e implementación del Modelo de Seguridad y Privacidad de la Información dispuesto por el Min TIC. Este modelo contempla un ciclo de operación que consta de cinco fases (componentes), las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información. A continuación, se describe cada uno de los componentes del ciclo:

1. Diagnóstico, en esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información. En la fase de diagnóstico se pretende alcanzar las siguientes metas:

   - Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la institución.
   - Determinar el nivel de madurez de los controles de seguridad de la información.
   - Identificar el avance de la implementación del ciclo de operación al interior de la institución.
   - Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
   - Identificación del uso de buenas prácticas en ciberseguridad.

2. Planificación, para el cual se deben utilizar los resultados de la etapa anterior y proceder a elaborar el Plan de Seguridad y Privacidad de la Información alineado con la plataforma estratégica de la institución, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo. En la fase de Planificación se pretende alcanzar las siguientes metas:

- Política de Seguridad y Privacidad de la Información
- Procedimientos de seguridad de la información
- Roles y responsabilidades de seguridad y privacidad de la información.
- Inventario de activos de información
- Integración del MSPI con el Sistema de Gestión Documental
- Identificación, valoración y tratamiento del riesgo
- Plan de comunicaciones
- Plan de diagnóstico de IPv4 a IPv6

3. Implementación: esta fase le permitirá a la Entidad, llevar acabo la implementación de la planificación realizada en la fase anterior del MSPI. En la fase de Implementación se pretende alcanzar las siguientes metas:

   - Planificación y Control Operacional
   - Implementación del plan de tratamiento de riesgos
   - Indicadores de gestión

4. Evaluación de desempeño: Se desarrolla con base en los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas. En la fase de evaluación del desempeño se pretende alcanzar las siguientes metas:

   - Plan de revisión y seguimiento, a la implementación del MSPI
   - Plan de ejecución de auditorías

5. Mejora continua: Consiste en consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones preventivas, correctivas y de mejora oportunas para mitigar las debilidades identificadas. En la fase de evaluación del desempeño se pretende alcanzar las siguientes metas:

- Plan de mejora continúa

4. OBJETIVOS.

4.1. OBJETIVO GENERAL

Fortalecer las capacidades institucionales para la identificación, gestión, tratamiento y mitigación de los riesgos de seguridad digital en las actividades institucionales en el entorno digital, en un marco de cooperación, colaboración y asistencia con los grupos de valor y grupos de interés.

4.2. OBJETIVOS ESPECÍFICOS.

- Definir las acciones a implementar en materia de seguridad y privacidad de la información basándose en los resultados del diagnóstico de la gestión de seguridad y privacidad de la información al interior de la institución y en el marco de la metodología de gestión del riesgo.

- Crear las condiciones para la gestión del riesgo de seguridad digital en los procesos y actividades institucionales generando confianza en el uso del entorno digital por parte de los grupos de valor y grupos de interés.

- Evaluar la efectividad, la eficiencia y la eficacia de las acciones implementadas en materia de seguridad y privacidad de la información para la mejora continua de las mismas.

5. ALCANCE

Para la implementación de la política de seguridad digital de la IUE, la Oficina de Informática como responsable de la misma, deberá desarrollar las siguientes acciones de gestión:

- Determinar el estado actual de los activos de información para la formulación del plan de tratamiento de riesgos de seguridad digital.

- Acompañar el diseño de una metodología de gestión de activos de información donde se tienen en cuenta aspectos como: cumplimiento legal, fechas de actualización de la clasificación, propietarios y criticidad de los activos. Asimismo, acompañar al área de gestión de archivo para aplicarla al crear y actualizar el inventario institucional de activos de información.

- Evaluar y ajustar la metodología institucional para la gestión de los riesgos de seguridad digital y el plan de tratamiento del riesgo

- Formular un plan de capacitación, sensibilización y comunicación de las políticas y buenas prácticas que mitiguen los riesgos de seguridad de la información a los que están expuestos los grupos de valor y grupos de interés

- Implementar acciones de mejora continua que permitan el cumplimiento del plan de tratamiento de riesgo de la seguridad digital

6. VIGENCIA

Anualmente la política de seguridad digital será revisada y evaluada en términos de ejecución y pertinencia; y de igual manera será validada o modificada para la entrada en vigencia de cada Plan de Desarrollo Institucional.

7. NORMAS DE REFERENCIA

El marco legal de la política de seguridad digital está constituido por las siguientes normas:

- Acuerdo 08 de 2019.
- Ley 1928 de 2018
- Acuerdo 02 de 2018
- Conpes 3854 de 2016. Política Nacional de Seguridad Digital
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Y especialmente en sus artículos a partir del 2.2.9.1.1.1. titulo 9. Define los lineamientos, instrumentos y plazos de la estrategia de gobierno en línea para garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones.
- Ley 1712 de 2014 - Transparencia y Acceso a la Información Pública. Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información púbica nacional y se dictan otras disposiciones.
- Ley estatutaria 1581 del 2012. Por la cual se dictan disposiciones generales para la protección de datos personales
- Decreto 103 de 2015. Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones (Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional).
- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la

Información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

8. DIAGNÓSTICO DAFP

El proceso de evaluación del desempeño institucional, llevado a cabo por medio del diligenciamiento de los formatos del FURAG 2 en la vigencia 2019, dio como resultado un Índice de Desempeño Institucional de 77,9. Al interior de éste índice, el puntaje de la política de seguridad digital se ubicó en 71,9.

Índice de desempeño institucional 2019

Puntaje de Política de Seguridad Digital

Fuente: Medición del Desempeño Institucional 2019