El futuro digital es de todos

MinTIC

Política Seguridad Digital

Política Seguridad Digital Generalidades

Entidad Líder: Ministerio de Tecnologías de la Información y Comunicaciones

Propósito

- Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país.

Marco Normativa

- Acuerdo 08 de 2019
- Ley 1928 de 2018
- Acuerdo 02 de 2018
- Conpes 3854 de 2016
- Decreto 1078 de 2015
- Ley 1712 de 2014 - Transparencia y Acceso a la Información Pública
- Ley estatutaria 1581 del 2012
- Decreto 103 de 2015
- Ley 1273 de 2009

Ámbito de aplicación

- Entidades que conforman la Administración Pública en los términos del artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas. La implementación de la Política de Gobierno Digital en las Ramas Legislativa y Judicial, en los órganos de control, en los autónomos e independientes y demás organismos del Estado, se realizará bajo un esquema de coordinación y colaboración armónica en aplicación de los principios señalados en los artículos 113 y 209 de la Constitución Política (Art. 2.2.9.1.1.2. - Decreto 1078 de 2015)

Atributos de calidad

- La adopción e implementación del Modelo de Gestión de Riesgos de Seguridad Digital, que será desarrollado y socializado por MinTic, por parte de las entidades y departamentos administrativos de la rama ejecutiva inicialmente, para los entes territoriales y demás partes interesadas, se adelantarán jornadas de sensibilización en temas de Seguridad Digital. Adicionalmente, Las entidades designadas, deberán dar cumplimiento a todas las actividades relacionadas en el plan de acción de seguimiento PAS del Conpes 3854 de 2016.

Política Seguridad Digital
Resultados Comparativos

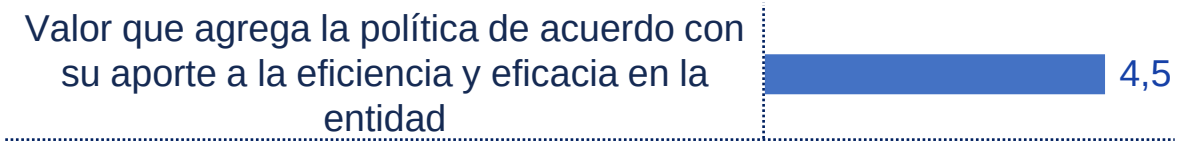
Con este índice se mide la capacidad de la entidad pública de identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en las actividades socioeconómicas de la entidad en un entorno digital y en un marco de cooperación, colaboración y asistencia, con el fin de contribuir al crecimiento de la economía digital nacional.

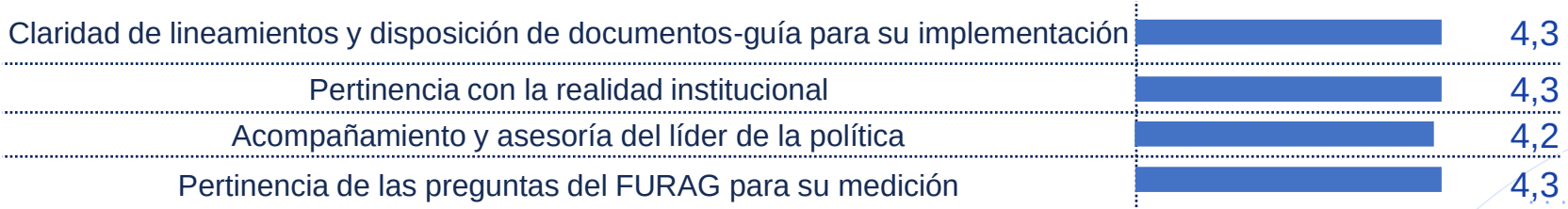
El índice de esta política ha mantenido un crecimiento durante las tres mediciones; a nivel nacional, fue más evidente el crecimiento que se dio en el año 2019 respecto al año 2018, cuando subió 4.2 puntos mientras que en la medición del 2020 mostró un incremento de 3.6. En territorio, el incremento en 2019 respecto a 2018 fue de 2.4 puntos y en 2020 respecto a 2019, fue de 1,4 puntos, manteniéndose relativamente constante dicho incremento.

Política Seguridad Digital
Percepción de las entidades
(valoración de 1 a 5)

El futuro digital es de todos | MinTIC

En **nación**, la percepción que tiene las entidades sobre la política de Seguridad Digital, es altamente favorable. De igual manera valoran positivamente el rol del líder, la aplicabilidad de la política y la pertinencia en su medición.

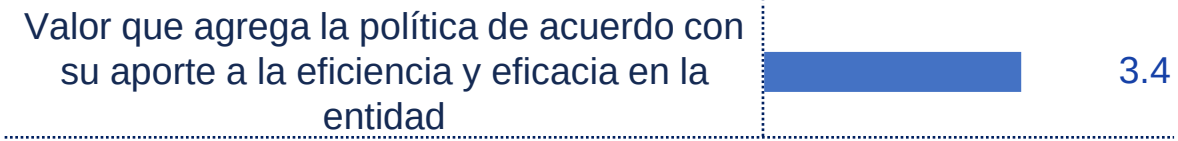




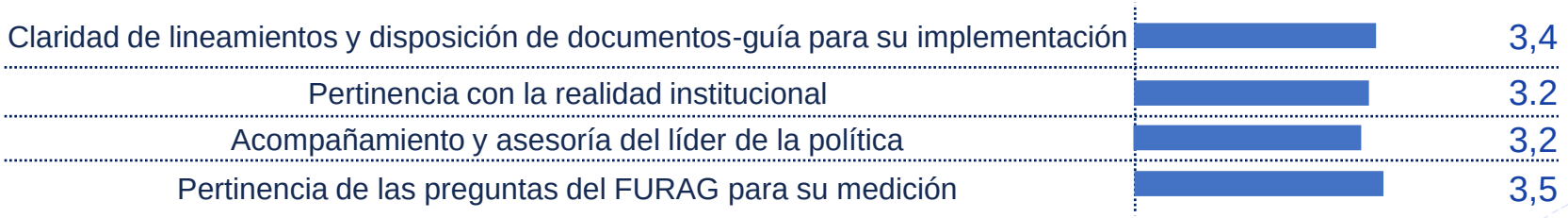
Política Seguridad Digital

Percepción de las entidades

(valoración de 1 a 5)



En **territorio**, la percepción que tiene las entidades sobre la política de Seguridad Digital, es modestamente favorable. De igual manera, valoran de manera modestamente favorable el rol del líder, la aplicabilidad de la política y la pertinencia en su medición.



Política Seguridad Digital
Recomendaciones para mejorar el desempeño
Entidades Nacionales

El futuro digital es de todos | MinTIC

- Fortalecer las capacidades en seguridad digital de la entidad a través de convenios o acuerdos de intercambio de información para fomentar la investigación, la innovación y el desarrollo de temas relacionados con la defensa y seguridad nacional en el entorno digital.
- Fortalecer las capacidades en seguridad digital de la entidad a través de ejercicios de simulación de incidentes de seguridad digital al interior de la entidad.
- Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como realizar la identificación anual de la infraestructura crítica cibernética e informar al CCOC.
- Realizar periódicamente ejercicios simulados de ingeniería social al personal de la entidad incluyendo campañas de phishing, smishing, entre otros, y realizar concientización, educación y formación a partir de los resultados obtenidos.
- Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como adoptar e implementar la guía para la identificación de infraestructura crítica cibernética.

Política Seguridad Digital
Recomendaciones para mejorar el desempeño
Entidades Nacionales

El futuro digital es de todos | MinTIC

- Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como participar en la contrucción de los planes sectoriales de protección de la infraestructura crítica cibernética.
- Realizar retest para verificar la mitigación de vulnerabilidades y la aplicación de actualizaciones y parches de seguridad en sus sistemas de información.
- Definir indicadores para medir la eficiencia y eficacia del sistema de gestión de seguridad y privacidad de la información (MSPI) de la entidad, aprobarlos mediante el comité de gestión y desempeño institucional, implementarlos y actualizarlos mediante un proceso de mejora continua.
- Cerciorarse de que los proveedores y contratistas de la entidad cumplan con las políticas de ciberseguridad internas.
- Identificar factores sociales que pueden afectar negativamente el cumplimiento de los objetivos institucionales. Desde el sistema de control interno efectuar su verificación.

Política Seguridad Digital
Recomendaciones para mejorar el desempeño
Entidades Territoriales

El futuro digital es de todos | MinTIC

- Fortalecer las capacidades en seguridad digital de la entidad a través de convenios o acuerdos de intercambio de información para fomentar la investigación, la innovación y el desarrollo de temas relacionados con la defensa y seguridad nacional en el entorno digital.
- Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como realizar la identificación anual de la infraestructura crítica cibernética e informar al CCOC.
- Realizar periódicamente ejercicios simulados de ingeniería social al personal de la entidad incluyendo campañas de phishing, smishing, entre otros, y realizar concientización, educación y formación a partir de los resultados obtenidos.
- Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como adoptar e implementar la guía para la identificación de infraestructura crítica cibernética.
- Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como participar en la construcción de los planes sectoriales de protección de la infraestructura crítica cibernética.
- Fortalecer las capacidades en seguridad digital de la entidad a través de ejercicios de simulación de incidentes de seguridad digital al interior de la entidad.

Política Seguridad Digital
Recomendaciones para mejorar el desempeño
Entidades Territoriales

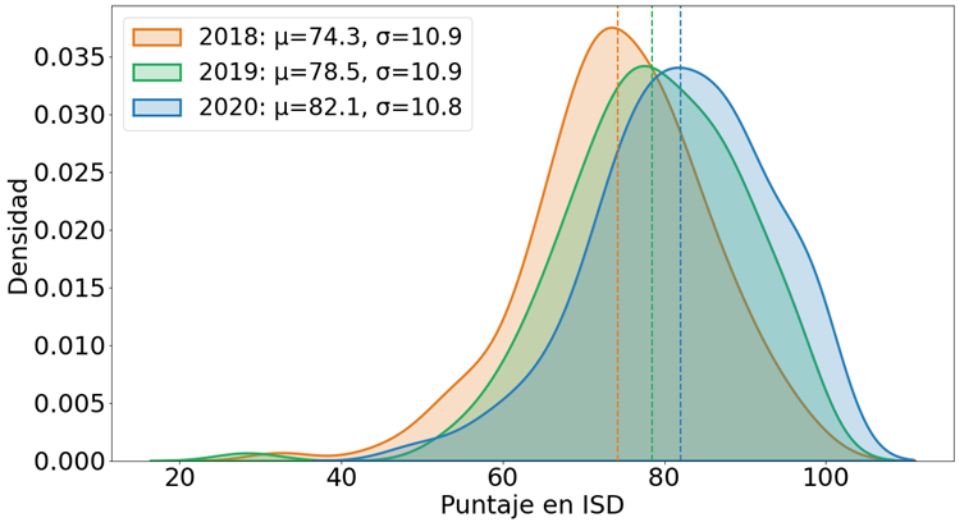
El futuro digital es de todos | MinTIC

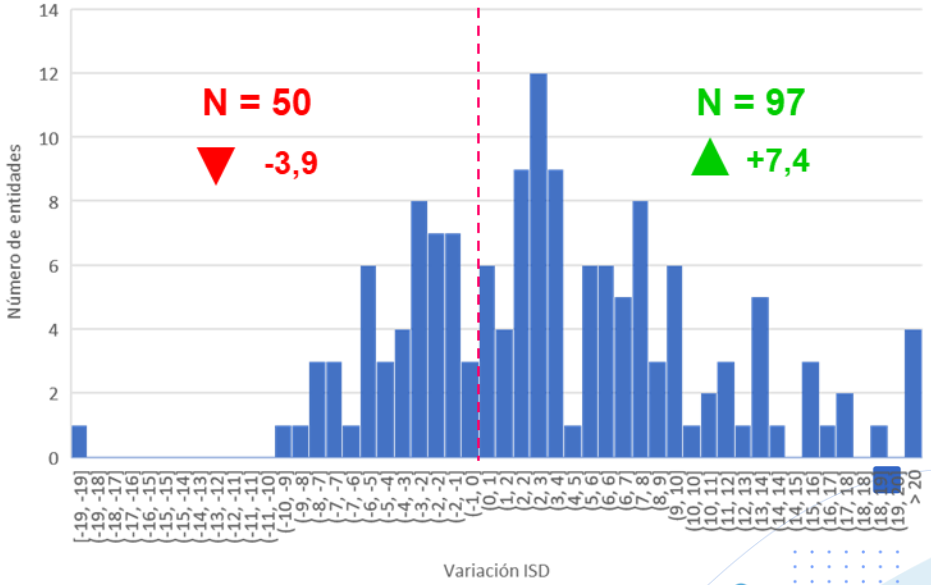
- Realizar retest para verificar la mitigación de vulnerabilidades y la aplicación de actualizaciones y parches de seguridad en sus sistemas de información.
- Definir indicadores para medir la eficiencia y eficacia del sistema de gestión de seguridad y privacidad de la información (MSPI) de la entidad, aprobarlos mediante el comité de gestión y desempeño institucional, implementarlos y actualizarlos mediante un proceso de mejora continua.
- Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en la entidad a partir de las necesidades identificadas, y formalizarlo mediante un acto administrativo.
- Utilizar técnicas de analítica de datos para predecir comportamientos o hechos de la entidad (analítica predictiva).
- Efectuar evaluaciones de vulnerabilidades informáticas.
- Establecer un procedimiento de gestión de incidentes de seguridad de la información, formalizarlo y actualizarlo de acuerdo con los cambios de la entidad.

II. Autoevaluación Líder Política Seguridad Digital

Índice de Seguridad Digital – Entidades nacionales

Índice de Seguridad Digital – Entidades nacionales



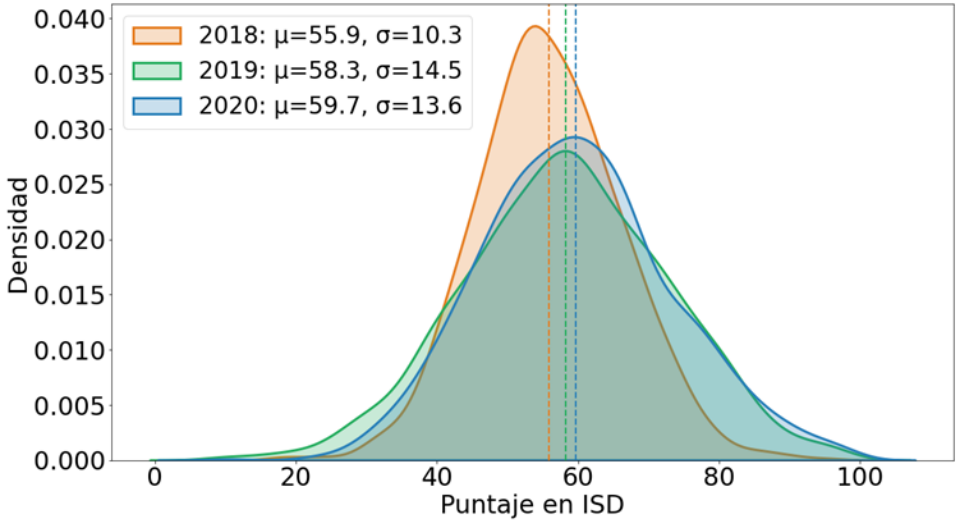


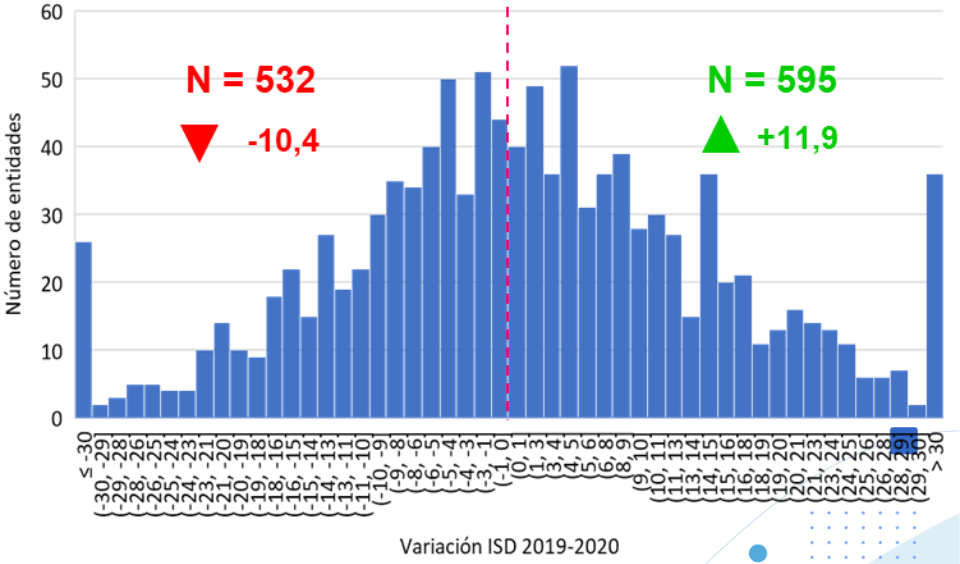
Índice de Seguridad Digital – Entidades nacionales

Principales avances	Principales oportunidades de mejora
- Destinación de recursos económicos y humanos que satisfagan las necesidades de seguridad de la información. - Clasificación y etiquetado de la información de acuerdo con las leyes aplicables vigentes. - Fortalecimiento de las capacidades en seguridad digital a través de su participación en las jornadas de sensibilización y capacitaciones del uso seguro de entorno digital convocadas por el Ministerio de Tecnologías de la Información y las Comunicaciones. - Definición del alcance del Sistema de Gestión de Seguridad de la Información (SGSI), aprobarlo mediante la alta dirección y actualizarlo de acuerdo con los cambios en el contexto. - Desarrollo de campañas de concientización en temas de seguridad de la información de manera frecuente y periódica, específicas para cada uno de los distintos roles dentro de las entidades.	- Fortalecer las capacidades en seguridad digital a través de convenios o acuerdos de intercambio de información para fomentar la investigación, la innovación y el desarrollo de temas relacionados con la defensa y seguridad nacional en el entorno digital. - Fortalecer las capacidades en seguridad digital a través de ejercicios de simulación de incidentes de seguridad digital. - Realizar la identificación anual de la infraestructura crítica cibernética e informar al CCOC. - Realizar periódicamente ejercicios simulados de ingeniería social incluyendo campañas de phishing, smishing, entre otros, y realizar concientización, educación y formación a partir de los resultados obtenidos. - Adoptar e implementar la guía para la identificación de infraestructura crítica cibernética.

Índice de Seguridad Digital – Alcaldías y Gobernaciones

Índice de Seguridad Digital – Entidades territoriales





Índice de Seguridad Digital – Entidades territoriales

Principales avances	Principales oportunidades de mejora
- Fortalecimiento de las capacidades en seguridad digital de las entidades a través de su participación en las jornadas de socialización y promoción del uso del modelo de gestión de riesgos de seguridad digital convocadas por el Ministerio de Tecnologías de la Información y las Comunicaciones. - Destinación de recursos económicos y humanos que satisfagan las necesidades de seguridad de la información. - Clasificación y etiquetado de la información de acuerdo con las leyes aplicables vigentes.	- Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital tales como realizar la identificación anual de la infraestructura crítica cibernética e informar al CCOC. - Fortalecer las capacidades en seguridad digital a través de convenios o acuerdos de intercambio de información para fomentar la investigación, la innovación y el desarrollo de temas relacionados con la defensa y seguridad nacional en el entorno digital. - Realizar periódicamente ejercicios simulados de ingeniería social incluyendo campañas de phishing, smishing, entre otros, y realizar concientización, educación y formación a partir de los resultados obtenidos. - Adoptar e implementar la guía para la identificación de infraestructura crítica cibernética. - Participar en la construcción de los planes sectoriales de protección de la infraestructura crítica cibernética.

CSIRT Gobierno - MinTIC

Catálogo de servicios

El futuro digital es de todos

MinTIC

Proactivos

1. Generación de Alertas y Advertencias de seguridad digital
2. Difusión de Información Relacionada con la Seguridad digital
3. Análisis de Vulnerabilidades Web
4. Monitoreo de eventos de seguridad de las Entidades de Gobierno
5. Monitoreo de disponibilidad de portales web de Entidades del Gobierno

Reactivos

6. Gestión de incidentes

Gestión de la seguridad

7. Capacitación y sensibilización en gestión de incidentes de Seguridad digital.

CSIRT

csirtgob@mintic.gov.co

018000910742 Opción: 4

El futuro digital es de todos

MinTIC

2021

Ministerio de Tecnologías de la Información y las Comunicaciones
Tel: +57(1) 344 34 60
Edificio Murillo Toro Cra. 8a entre calles 12A y 12B,
Bogotá, Colombia - Código Postal 111711
www.mintic.gov.co