Unidades Tecnológicas de Santander

Un buen presente , un mejor futuro

Política Nacional de Seguridad Digital

@VIVEUTS
UNIDADES TECNOLÓGICAS DE SANTANDER
/VIVEUTS
UNIDADESUTS
WWW.UTS.EDU.CO

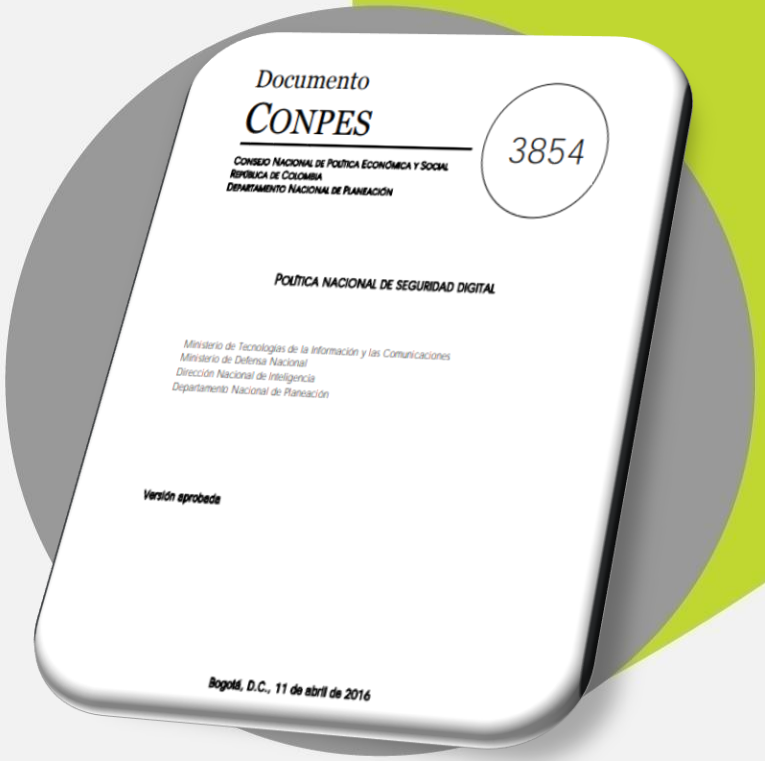
Capacitación No 04

Dirección Administrativa de Talento Humano

Recordemos…..

¿Qué es un Documento Conpes?

Conpes es la sigla que hace referencia al Consejo Nacional de Política Económica y Social. Ésta es la máxima autoridad nacional de planeación y se desempeña como organismo asesor del Gobierno en todos los aspectos relacionados con el desarrollo económico y social del país. Este Consejo aprueba documentos que son el instrumento técnico de apoyo y coordinación en la formulación de las políticas. Es decir, donde se definen las acciones para responder a los retos del país.



¿Qué es un Conpes en Colombia?

Ésta es la máxima autoridad nacional de planeación y se desempeña como organismo asesor del Gobierno en todos los aspectos relacionados con el desarrollo económico y social del país, fue creado por la Ley 19 de 1958.

Política Nacional de Seguridad Digital (Conpes 3854)

La Política Nacional de Seguridad Digital (Conpes 3854 de 2016) es una hoja de ruta para que el Gobierno, las organizaciones públicas y privadas, la fuerza pública, la academia y los ciudadanos en general, cuenten con un entorno digital confiable y seguro. Esta articula una visión estratégica que pretende que los colombianos hagan un uso responsable del entorno digital y fortalezcan sus capacidades para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital.

¿Cuál es el objetivo Política Nacional de Seguridad Digital?

El objetivo general de esta política es que los ciudadanos las entidades del Gobierno y los empresarios conozcan e identifiquen los riesgos a los que están expuestos en el entorno digital y aprendan cómo protegerse, prevenir y reaccionar ante los delitos y ataques cibernéticos.

La idea es educar y fomentar una cultura en todos seamos conscientes de que el manejo del riesgo es nuestra responsabilidad. Por ejemplo, desde la perspectiva de los ciudadanos, no dándole sus claves a nadie, utilizando contraseñas de alta seguridad y cambiándolas periódicamente, no dejando el correo abierto en sitios públicos, tener cuidado con los correos spam, entre otros cuidados.

¿En qué se basa la Política Nacional de Seguridad Digital?

Se basa en unos principios fundamentales, que contemplan: salvaguardar los derechos humanos y los valores fundamentales de los individuos, adoptar un enfoque incluyente y colaborativo, asegurar una responsabilidad compartida entre todos los actores involucrados y adoptar un enfoque basado en riesgos, que permita a los individuos el libre, confiable y seguro desarrollo de sus actividades en el entorno digital.

¿Esta Política tiene componentes educativos, de libre acceso, culturales, incluyentes y penales?

Si, la Política contempla la realización de campañas educativas y de concientización para que los colombianos conozcan cuáles son los riesgos a los que están expuestos con el uso del internet, cómo cuidarse y prevenir los delitos y ataques cibernéticos. De hecho, el Ministerio TIC implementa la iniciativa En TIC confío, que es la estrategia de promoción de uso responsable de internet y de las nuevas tecnologías.

¿Esta Política de Seguridad Digital limita la libertad de expresión?

No. La nueva Política Pública de Seguridad Digital debe ser implementada y compatible con la libertad de expresión, el libre flujo de la información, la confidencialidad de la información, la protección de la privacidad y los datos personales.

¿Por qué la implementación de la Política mejoraría la economía del país?

Con un ambiente digital seguro se podrá garantizar la prosperidad económica y social, ya que con ello los ciudadanos perderán el temor a realizar compras y tramites en línea, transacciones de gobierno electrónico, entre otras actividades que contribuyan al crecimiento económico del país.

Con la implementación de la Política de Seguridad Digital las entidades públicas y privadas deben adoptar estos nuevos modelos, generándose entre los años 2016 al 2020 cerca de 307.000 empleos de acuerdo a un estudio realizado por la Comisión de Regulación de Comunicaciones (CRC) de Colombia, con apoyo de la Dirección de Estudios Económicos del Departamento Nacional de Planeación.

Estrategias de la Política de Seguridad Digital

1. Establecer un marco institucional claro en torno a la seguridad digital, basado en la gestión de riesgos.
2. Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital.
3. Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos.
4. Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos.
5. Generar mecanismos permanentes y estratégicos para impulsar la cooperación,colaboración y asistencia en seguridad digital, a nivel nacional e internacional

CONPES 3854 de 2016

¿La Política de Seguridad Digital da la autoridad al Gobierno para regular las redes sociales?

No, el Gobierno Nacional no censura el uso de las redes sociales, por el contrario promueve el uso seguro y responsable del internet.

La Política abre el espacio para adelantar un debate sobre cómo deberían abordarse el tema de balances entre derechos y los delitos digitales. Por eso es fundamental un debate en el que se integren todas las partes interesadas.

Como efecto de las discusiones se generarán las medidas que sean necesarias para promover un ambiente digital más confiable y seguro.

¿Cómo se puede proteger un ciudadano en el ciberespacio?

El tema de seguridad es responsabilidad de todos los ciudadanos. Cada persona, empresa o entidad del Gobierno debe velar por su seguridad y proteger su información en el mundo digital. Algunas recomendaciones son:

- ✓ No descargar archivos sospechosos.
- ✓ Actualizar el software del sistema periódicamente.
- ✓ Usar antivirus y aplicaciones anti-malware.
- ✓ Crear mejores contraseñas y cambiarlas cada seis meses.
- ✓ Acostumbrar a cerrar las sesiones al terminar.
- ✓ Evitar operaciones privadas en redes abiertas y públicas.
- ✓ Desconectarse de internet cuando no se necesite.
- ✓ Realizar copias de seguridad.
- ✓ Navegar por páginas web seguras y de confianza.
- ✓ Comprobar la seguridad de la red WIFI.
- ✓ No hacer clic en enlaces raros.
- ✓ No dar datos personales a desconocidos.
- ✓ En las empresas se debe hacer una política de seguridad corporativa.

¿Dónde puedo denunciar los delitos cibernéticos?

Si un ciudadano es víctima de delitos electrónicos financieros podrá denunciar en el CAI Virtual de la Policía Nacional. Con los soportes respectivos, los ciudadanos deben acudir a las entidades financieras, donde deben gestionar la denuncia y si considera que su solicitud no ha sido tramitada adecuadamente podrá recurrir a la Superintendencia Financiera de Colombia, donde estudiarán el caso y tendrá mayor probabilidad de recuperar el dinero hurtado.

Fiscali

Si el ciudadano es víctima de otros tipos de delitos informáticos, la autoridad competente en Colombia para conocer de estos casos es el Centro Cibernético Policial -CCP- de la Policía Nacional, encargado de la ciberseguridad, y de ofrecer información, apoyo y protección ante los delitos cibernéticos.

Esta autoridad desarrolla labores de prevención, atención, investigación y judicialización de los delitos informáticos en el país. Puede hacer la denuncia en el CAI Virtual, en la página web https://caivirtual.policia.gov.co

Material de Apoyo para Estudio

- Política Nacional de Seguridad Digital Conpes 3854 de 2016
- Video No 01 En que consiste el Programa en TIC confió
- Video No 02 Seguridad Digital Conpes que protege a los Ciudadanos
- Video No 03 Ciberseguridad y Ciberdefensa - Política Nacional de Seguridad Digital (CONPES 3854)
- Manual Procedimiento para la Protección de Datos Personales UTS
- Lineamientos para la Gestion de Riesgos de Seguridad Digital en las Entidades Publicas

Click aquí para responder el Test de lo Aprendido

DIRECCIÓN ADMINISTRATIVA DE TALENTO HUMANO

Unidos por la Acreditación