Unidades Tecnológicas de Santander

¡Lo hacemos posible!

SEGURIDAD DIGITAL Y GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

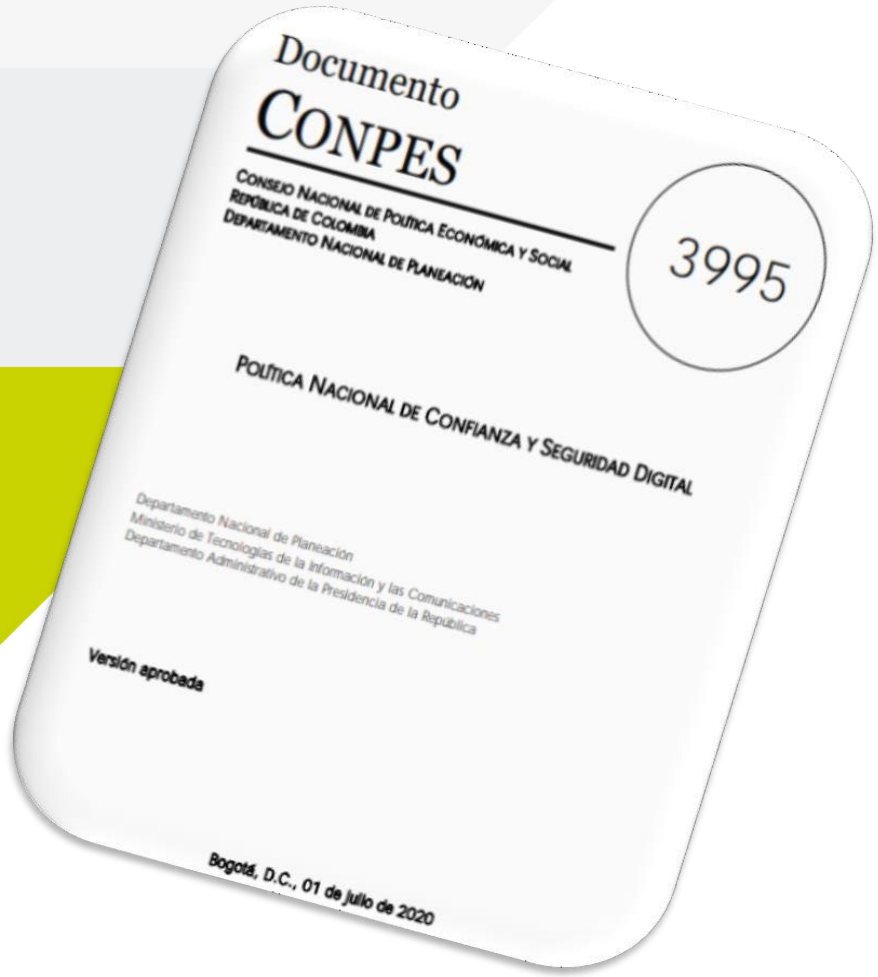
Febrero del 2023

Dirección Administrativa de Talento Humano

Sonnia Yaneth García Benítez
Directora Administrativa de Talento Humano

Unidades Tecnológicas de Santander
¡Lo hacemos posible!

POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL (CONPES 3995)



La Política Nacional de Confianza y Seguridad Digital (Conpes 3995 de 2020), tiene por objetivo establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

¿Cuál es el objetivo Política Nacional de Confianza y 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 que 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.

Unidades Tecnológicas de Santander

¡Lo hacemos posible!

¿Qué es Confianza Digital?

El Conpes la define como “la probabilidad suficiente alta de que un actor externo realice una acción que es beneficiosa (o al menos no perjudicial) para nosotros, de forma que se considere una cooperación con dicho actor” y además como “la base de todas y cada una de las interacciones en el futuro digital”. Con base en estas definiciones, es válido afirmar que, sin confianza digital, las personas no proporcionarán su información a las plataformas digitales, ergo, el intercambio de bienes y servicios se verá limitado y a su vez las dinámicas de Comercio Electrónico.

RESOLUCIÓN 500 DE 2021, “POR LA CUAL SE ESTABLECEN LOS LINEAMIENTOS Y ESTÁNDERES PARA LA ESTRATEGIA DE SEGURIDAD DIGITAL

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) expide la 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".

Esta resolución tiene por objetivo establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI y la guía de gestión de riesgos de seguridad de la información y el procedimiento para la gestión de los incidentes de seguridad digital. Asimismo, establece las directrices y estándares para la estrategia de seguridad digital.

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.

Unidades Tecnológicas de Santander

¡Lo hacemos posible!

¿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.

uts

¿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

Unidades Tecnológicas de Santander

¡Lo hacemos posible!

Material de Apoyo para Estudio

- ✓ Documento CONPES 3854 de 2016,
- ✓ Documento CONPES 3995 (2020).
- ✓ Documento CONPES 3885 (2020) pp. 27
- ✓ RESOLUCIÓN 500 LINEAMIENTOS Y ESTÁNDARES PARA LA ESTRATEGIA DE SEGURIDAD DIGITAL
- ✓ RESOLUCIÓN NÚMERO 2256 SE ACTUALIZA LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
- ✓ RESOLUCIÓN 924 SE ACTUALIZA LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES
- ✓ MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
- ✓ 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)
- ✓ Lineamientos para la Gestion de Riesgos de Seguridad Digital en las Entidades Públicas
- ✓ ACUERDO POLÍTICA DE TRATAMIENTO DE LA INFORMACIÓN UTS

¡Gracias!

uts Unidades Tecnológicas de Santander

¡Lo hacemos posible!