PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LAS UNIDADES TECNOLÓGICAS DE SANTANDER

Presentado Por:

Coordinador Recursos Informáticos

UNIDADES TECNOLOGICAS DE SANTANDER

BUCARAMANGA, FEBRERO DE 2019

**Plan de Seguridad y Privacidad de la información de las Unidades Tecnológicas de Santander**

OBJETO: Crear mediante la articulación de los sistemas de Gestión de la Institución mediante la implementación de políticas, controles y procedimientos que permitan, medir, prevenir y atender la atención de riesgos en la seguridad y privacidad de la información en la Institución.

ALCANCE: El Alcance de la Política de seguridad y privacidad de la información en la Institución enmarcado en la estrategia de Gobierno en Línea, comprende todas las oficinas tanto administrativas cómo académicas de la institución, sus servidores públicos, docentes y contratistas para el manejo de la información de la Institución.

POLITICA INSTITUCIONAL

Para las Unidades Tecnológicas de Santander la información constituye un activo valioso para la gestión, control y toma de decisiones de todas sus actividades misionales.

PARAMETROS DE LA POLITICA

PROPIEDAD DE LA INFORMACIÓN: Las Unidades Tecnológicas de Santander tiene la propiedad absoluta de la información generada y gestionada en la institución por parte de los servidores, contratistas y docentes, garantizada en acuerdos de confidencialidad y manejo de la información para garantizar el buen uso de acuerdo a sus funciones y obligaciones en las labores operativas y de conservación de las misma, sin perjuicio para la Institución de perder la propiedad de la Información.

GESTION DE ACTIVOS DE INFORMACION: Se entenderá cómo activo de información, todo documento u archivo físico, electrónico o digital, que tiene valor para el ejercicio propio de la misión de la Institución, para lo cual el Grupo de Recursos Informáticos será la responsable de Inventariar los activos de información según su categoría y uso, determinando el proceso responsable y los posibles riesgos asociados al manejo de estos activos, protegiéndolos según la determinación de los planes de riesgos que se establezcan pare este fin.

CONTROL DE ACCESO: Las Unidades Tecnológicas de Santander, por medio de la oficina de Recursos Informáticos establecerán los controles de acceso a la información necesarios en los equipos, sistemas de información, redes internas y otros activos de información que lo requieran.

ADMINISTRACION DE REDES Y EQUIPOS: Los equipos de cómputo, sistemas de almacenamiento y procesamiento de datos, redes de datos son herramientas de apoyo para la ejecución de labores de servidores y contratistas tanto administrativos cómo académicos, por lo tanto la Oficina de Recursos Informáticos, cómo administradora de la infraestructura tecnológica dispondrá de los lineamientos necesarios para garantizar la disponibilidad, soporte y mantenimiento de los equipos y redes de la Institución.

USO DE SOFTWARE Y SISTEMAS DE INFORMACION, CORREO ELECTRONICO Y USO DE INTERNET: Todos los funcionarios tanto de planta como contratista de la Institución son responsables del buen uso del software, sistemas de información, correo electrónico y uso del internet, respetando la legalidad del software, evitando instalar software no licenciado en los equipos, todas las herramientas de correo electrónico, internet que provee o delega la Institución deberá sólo ser usado con fines institucionales evitando cualquier uso de interés personal.

RESPONABILIDADES: Todos los funcionarios tantos de planta como contratista de la Institución a los cuales les sean asignados usuarios de acceso a sistemas de Información, tendrán el uso y resguardo de los mismos, asumiendo la responsabilidad de los roles y permisos de dicho usuario y contraseña asignada, evitando su préstamo, divulgación y uso indebido de los activos de información a los cuales tenga acceso.

SEGURIDAD FISICA DE LA INFORMACION: Las Unidades Tecnológicas de Santander mediante la oficina de Recursos Informáticos determinará las áreas donde reposen los activos de información, planteando planes para impedir el acceso no autorizado, evitar robo, pérdida, daño entre otros que puedan afectar la integridad de los activos de información, sistemas de procesamiento y comunicaciones de la institución.