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

Presentado Por:
Coordinador Recursos Informáticos

UNIDADES TECNOLÓGICAS DE SANTANDER

BUCARAMANGA, ENERO DE 2024

Tabla de contenido

1 OBJETIVO

Establecer un Plan de Seguridad y Privacidad de la Información que apoye el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información de las UTS, alineadas con la NTC/IEC ISO 27001:2022, la estrategia de gobierno digital, la Política de Seguridad de la Información y la Política de Administración del Riesgo de las UTS, en cumplimiento de las disposiciones legales vigentes.

2 ALCANCE

El alcance del Plan de Seguridad y Privacidad de la Información de las Unidades Tecnológicas de Santander, aplica para todos los procesos, funcionarios, proveedores, contratistas, docentes y comunidad en general, que en razón del cumplimiento de sus funciones, compartan, utilicen, recolecten, procesen, intercambien o consulten información, así como a los entes de control o entidades que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación.

3 TÉRMINOS Y DEFINICIONES

Activo de Información: Conocimientos o datos que tienen valor para la Institución.

Información: Todo aquel conjunto de datos organizados en poder de una entidad que sean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

Seguridad de la Información: Es la preservación de la Confidencialidad, Integridad y Disponibilidad de la información Institucional para propender por la autenticidad, trazabilidad, no repudio y fiabilidad de la misma.

Riesgo de Seguridad de la Información: Posibilidad que una amenaza dada explote vulnerabilidades de un activo o de un grupo de activos y por lo tanto cause daño a la Institución.

Integridad: Propiedad de salvaguardar la exactitud y completitud de los activos

Sistema de Gestión: Marco de políticas, procedimientos, guías y recursos asociados para lograr los objetivos de la Institución.

Políticas: Intenciones globales y orientación tal como se expresan formalmente por la dirección.

Procedimiento: Forma especificada para llevar a cabo una actividad o un proceso

Registro: Documento que presenta resultados obtenidos o proporciona evidencias de actividades desempeñadas

4 METODOLOGÍA IMPLEMENTACIÓN MODELO DE SEGURIDAD

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las Unidades Tecnológicas de Santander puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

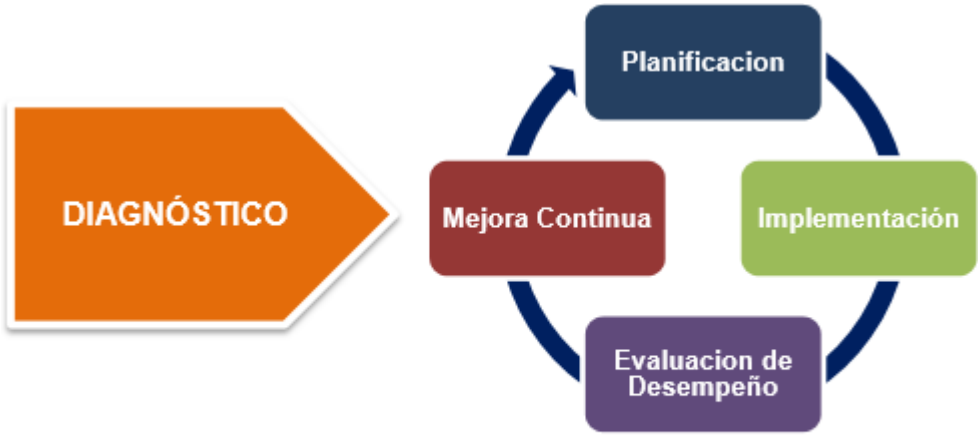
Fase Diagnostico: Permite identificar el estado actual de la institución con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información

Fase Planificación (Planear): En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.

Fase Implementación (Hacer): En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.

Fase Evaluación de desempeño (Verificar): Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.

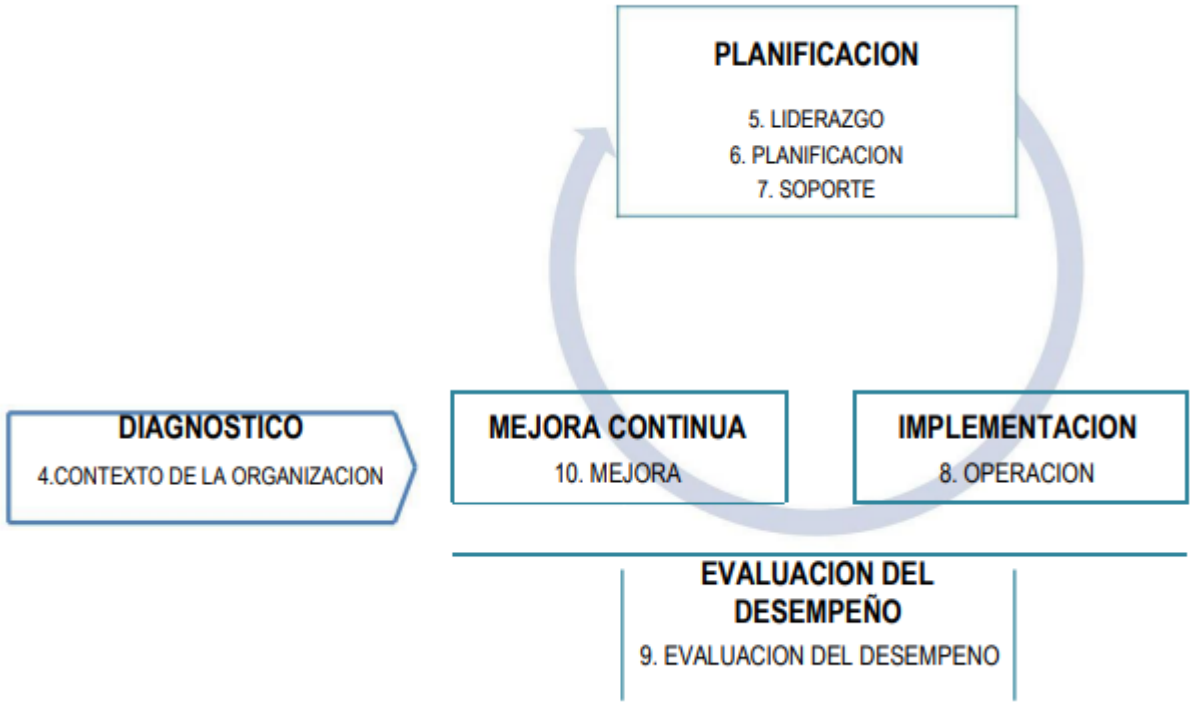
Fase Mejora Continua (Actuar): Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones



Ciclo de operación del Modelo de Seguridad y Privacidad de la Información
Fuente: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

4.1 ALINEACIÓN NORMA ISO 27001:2022 VS CICLO DE OPERACIÓN

Aunque en la norma ISO 27001:2022 no se determina un modelo de mejora continua (PHVA) como requisito para estructurar los procesos del Sistema de Gestión de Seguridad de la Información, la nueva estructura de esta versión se puede alinear con el ciclo de mejora continua de las modelos de gestión de la siguiente forma:



Fase DIAGNOSTICO en la norma ISO 27001:2022. En el capítulo 4 - Contexto de la organización de la norma ISO 27001:2022, se determina la necesidad de realizar un análisis de las cuestionas externas e internas de la organización y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesadas de la organización en el alcance del SGSI.

Fase PLANEACIÓN en la norma ISO 27001:2022 En el capítulo 5 - Liderazgo, se establece las responsabilidades y compromisos de la Alta Dirección respecto al Sistema de Gestión de Seguridad de la Información y entre otros aspectos, la necesidad de que la Alta Dirección establezca una política de seguridad de la información adecuada al propósito de la organización asegure la asignación de los recursos para el SGSI y que las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen. En el capítulo 6 - Planeación, se establece los requerimientos para la valoración y tratamiento de riesgos de seguridad y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento. En el capítulo 7 - Soporte se establece que la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua Sistema de Gestión de Seguridad de la Información.

Fase IMPLEMENTACIÓN en la norma ISO 27001:2022. En el capítulo 8 - Operación

de la norma ISO 27001:2022, se indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

Fase EVALUACIÓN DEL DESEMPEÑO en la norma ISO 27001:2022. En el capítulo 9 - Evaluación del desempeño, se define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información.

Fase MEJORA CONTINUA en la norma ISO 27001:2022. En el capítulo 10 - Mejora, se establece para el proceso de mejora del Sistema de Gestión de Seguridad de la Información, que a partir de las no-conformidades que ocurran, las organizaciones deben establecer las acciones más efectiva para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan.

4.2 Situación Actual

ÁMBITO	SITUACIÓN ACTUAL
Diagnóstico de seguridad y Privacidad	Las Unidades Tecnológicas de Santander cuenta con un instrumento de evaluación de la implementación del modelo de seguridad y privacidad de la información. Este instrumento de Evaluación cuenta el resultado de identificar el nivel de madurez de la Seguridad y Privacidad de la Información en la entidad, identificar las vulnerabilidades técnicas y administrativas y generar planes de mejoramiento para subsanar dichas vulnerabilidades
Plan de Seguridad y privacidad	Es necesario fortalecer los procesos y procedimientos que hacen referencia a la implementación de la seguridad y privacidad de la información en las Unidades Tecnológicas de Santander, actividad que debe ser liderada por el Grupo de Recursos Informáticos, Asesorada por la oficina de Planeación.
	Se deben establecer políticas del tratamiento de riesgos y revisión en un periodo adecuado, reformando el modelo de manejo de incidentes de seguridad para ser elaborado con las especificaciones adecuadas**.**

5 PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Con el objetivo de la entidad de implementar el sistema de gestión de seguridad de la información- SGSI se definieron las siguientes actividades para el 2024 con las cuales se establece el plan de seguridad y privacidad de la información.

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLES	FECHAS PROGRAMACIÓN
ACTIVOS DE LA INFORMACIÓN	Levantamiento Activos de Información	Actualización de Activos previamente identificados y valorados	Grupo de recursos informáticos	Marzo 2024
GESTIÓN DE RIESGOS	Revisión de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	Grupo de recursos informáticos	Abril 2024

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLES	FECHAS PROGRAMACIÓN
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital	Identificación, Análisis y Evaluación de Riesgos Seguridad y Privacidad de la Información, Seguridad Digital	Grupo de recursos informáticos	Abril 2024
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Grupo de recursos informáticos	Mayo 2024
	Publicación	Publicación Matriz de riesgos a nivel Institucional	Grupo de recursos informáticos	Mayo 2024
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Grupo de recursos informáticos	Cuatrimestral
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Seguimiento de incidentes de seguridad de la información	Seguimiento de incidentes de seguridad de la información	Grupo de recursos informáticos	Cuatrimestral
	Gestionar los incidentes de Seguridad de la Información identificado	Gestionar los incidentes de seguridad de la información de acuerdo a lo establecido en el procedimiento definido.	Grupo de recursos informáticos	Anual
PLAN DE CONTINUIDAD	Revisión y Actualización del Plan de Continuidad	Revisión y Actualización del Plan de Continuidad	Grupo de recursos informáticos	Anual
VULNERABILIDADES	Ejecutar pruebas de vulnerabilidades y pentest	Ejecución de las pruebas de vulnerabilidades y pentest de acuerdo al alcance y la metodología establecida	Grupo de recursos informáticos	Septiembre 2024
PROTECCIÓN DE DATOS PERSONALES	Revisión de bases de datos	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos	Grupo de recursos informáticos	Anual
	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información.	Grupo de recursos informáticos	Anual

6 MARCO NORMATIVO

- Constitución Política de Colombia. Artículo 15.
- Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).
- Ley 527 de 1999. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.
- Ley 850 de 2003. Por medio de la cual se reglamentan las veedurías ciudadanas
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Decreto 1008 del 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Resolución 2999 del 2008. Por el cual se adoptan las políticas de seguridad para el manejo de la información y se dictan otras normas para el uso y administración de los bienes y servicios informáticos del Ministerio TIC.
- Resolución 2034 de 2016. Por la cual se adoptó el Modelo de Responsabilidad Social Institucional en el Ministerio TIC.
- Resolución 2007 de 2018. Por la cual se actualiza la política de tratamiento de datos personales del Ministerio/Fondo TIC.
- Resolución 911 de 2018. Por la cual se actualiza el Modelo Integrado de Gestión del MinTIC.
- Resolución 2133 de 2018. Por la cual se establecen las condiciones especiales del Teletrabajo en el Ministerio de Tecnologías de la Información y las Comunicaciones, y se deroga las resoluciones No 3559 y 4950 de 2022, 2313 y 494 de 2014 y 2787 de 2016.
- Resolución 512 de 2019. Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital