LINEAMIENTOS PARA LA IMPLEMENTACIÓN DE UN SGSI A PARTIR DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

Garantizar la continuidad de los procesos y servicios asegurando los datos en la CAS Santander.

Descripción breve

Implementar formalmente un SGSI, es un proceso que con lleva tiempo, recursos, y disposición y conciencia que asegurar los datos generados en los diferentes procesos estratégicos, misionales y operativos es un factor de competitividad de las entidades territoriales y así garantizar la continuidad de los servicios y la transparencia del accionar de las mismas.

Tabla de contenido

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, MSPI, PARA LA CAS SANTANDER.

1 Introducción, ¿Qué es el MSPI?

De acuerdo a los lineamientos establecidos en la política de Gobierno Digital del MINTIC, el Modelo de Seguridad y Privacidad de la Información (MSPI) es una iniciativa del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) de Colombia, que proporciona lineamientos a las entidades públicas para la adopción de *buenas prácticas* en seguridad de la información. Este modelo se basa en estándares internacionales y busca orientar la gestión adecuada del ciclo de vida de la seguridad de la información, abarcando las fases de planeación, implementación, evaluación y mejora continua.

Su objetivo principal es garantizar la confidencialidad, integridad, disponibilidad y privacidad de los datos en las entidades públicas, asegurando que la seguridad de la información esté integrada en todos los procesos, trámites, servicios y sistemas de información.

En síntesis, **El MSPI,** tiene como finalidad que las entidades públicas incorporen la seguridad de la información en todos sus procesos y activos, con el fin de:

- Preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.
- Orientar la gestión adecuada del ciclo de vida de la seguridad de la información.
- Habilitar la implementación de la Política de Gobierno Digital.

La Corporación Autónoma Regional de Santander (CAS) ha definido su política de seguridad de la información, la cual está disponible en su sitio web oficial, este documento aborda aspectos clave como:

- **Objetivos de Seguridad:** Establece los objetivos que la entidad busca alcanzar en términos de protección de la información.
- **Alcance:** Define los ámbitos y procesos a los que se aplica la política.
- **Roles y Responsabilidades:** Detalla las responsabilidades de los empleados y áreas en relación con la seguridad de la información.
- **Directrices Generales:** Proporciona lineamientos sobre cómo se debe manejar la información, incluyendo su clasificación, almacenamiento, transmisión y eliminación.
- **Cumplimiento Legal:** Asegura que la entidad cumple con las normativas y leyes vigentes relacionadas con la protección de datos y la seguridad de la información.

Este documento pretende no solo recomendar se hagan los respectivos ajustes al documento de política hoy vigente, busca que se establezca una organización para la Gobernanza del MSPI, y con base en la planificación del modelo MSPI se defina un plan de implementación que incluya la asignación de recursos, la definición de un cronograma y la designación de responsables para garantizar la efectiva aplicación del sistema de gestión de la seguridad de la información en la organización.

Es importante recordar que este plan debe cumplir con una metodología tipo PHVA, que permita avanzar desde una planificación cuyo objetivo primordial es la protección de la información, (conservando atributos de Confidencialidad, Disponibilidad, integridad y oportunidad) y la continuidad del negocio desde el punto de vista de la responsabilidad del área de tecnología.

Por lo tanto, es importante avanzar en ciclos cortos que incluyen la mejora continua permanente hasta llegar a un modelo maduro que incluya no solo el cumplimiento normativo, si no la madurez de la entidad en la importancia de cumplir los lineamientos y procedimientos asociados al modelo MSPI. Ahora, el desarrollo del plan debe incluir a todo el personal que tiene relación con la CAS, funcionarios de todos los niveles, contratistas, proveedores y comunidad en general, lo que implica que el plan tiene un componente amplio de concientización y formación para lograr los objetivos primordiales establecidos.

Este documento recomienda la implementación de un plan para materializar los lineamientos del modelo de seguridad y privacidad de la información, conocido como implementación de un Sistema de Gestión de Seguridad de la Información, SGSI, igualmente recomienda actualizar el actual documento de Política de Seguridad de la información publicado y vigente, para que así, la CAS Santander pueda avanzar gradualmente en la implementación bajo un modelo soportado en políticas, procesos y procedimientos, que le permita ir interiorizando y aplicando en el día a día las buenas prácticas para lograr los objetivos primordiales, que son:

- **Protección de la información**, que se encuentra en activos de información digitales y no digitales de la entidad.
- **Garantizar la continuidad del negocio de la CAS Santander** desde el punto de vista de la responsabilidad de la oficina de Gestión de Información ambiental y sistemas de apoyo.

Para establecer el plan se debe seguir una estructura metodológica alineada con los lineamientos y normas del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), así como las normativas relacionadas con la Gobernanza Digital en el país, en especial el Decreto 1008 de 2018 y el Marco de Referencia de Arquitectura TI.

2 Ajustes recomendados para actualizar el documento de política de seguridad y privacidad de la información.

Con base en el análisis realizado al documento de política de seguridad de la información, publicado en la sede electrónica de la CAS Santander, es recomendable hacer los ajustes que se relacionan a continuación, los cuales están alineados a un modelo de buenas practicas definidos por la norma ISO/IEC-27001, esto con el fin de fortalecer dicho documento y así avanzar sobre la iniciativa de implementar un Sistema de Gestión de la Seguridad de la Información, SGSI. Las recomendaciones se toman con base en la etapa de Planear que define dicha norma, ese análisis es el siguiente:

2.1 Alcance de la política.

El documento **define su alcance** de manera general al establecer que las políticas de seguridad de la información son aplicables a:

- Todos los funcionarios de la Corporación Autónoma Regional de Santander (CAS).
- Los contratistas y terceros que manejan o tienen acceso a los activos de información de la entidad.
- Los procesos, sistemas y recursos de tecnología involucrados en la gestión de información.

Adicionalmente, menciona que el alcance incluye todos los activos de información asociados a la gestión ambiental en los municipios de Santander donde opera la CAS.

No obstante, se podría mejorar especificando los límites exactos de aplicación (por ejemplo, procesos específicos o sistemas críticos) para evitar ambigüedades y asegurar claridad para los involucrados.

De acuerdo a lo identificado en el documento a continuación, se propone modificar la actual política de seguridad vigente considerando los aspectos que se enumeran a continuación.

2.1.1 Definición del alcance de la política.

Para especificar los **límites exactos de aplicación** en el alcance de la política de seguridad de la información, es importante que estos sean claros, medibles y específicos, para garantizar que todos los involucrados comprendan hasta dónde llega su responsabilidad. A continuación, se presentan los aspectos clave a considerar para establecer estos límites:

2.1.1.1 *Definir los Activos de Información Involucrados*

- **Qué incluir:** Determinar cuáles activos de información (documentos, bases de datos, sistemas, aplicaciones, servidores, etc.) están protegidos por la política.
- **Cómo especificarlo:** Listar explícitamente los activos o agruparlos en categorías, por ejemplo:
    - Sistemas críticos: Plataforma de la sede electrónica, sistema financiero, sistema de gestión ambiental.
    - Documentos sensibles: Registros de usuarios, reportes ambientales, bases de datos de usuarios, y demás información clasificada.

2.1.1.2 *Alcance Organizacional*

- **Qué incluir:** Especificar qué áreas, departamentos o roles dentro de la entidad deben acatar la política.
- **Cómo especificarlo:** Detallar qué unidades funcionales están cubiertas, como:
    - Todos los departamentos de la CAS que producen o usan información ambiental.
    - Contratistas y proveedores que accedan a sistemas de la entidad.
    - Personal administrativo y técnico con acceso a información sensible.

2.1.1.3 *Cobertura Geográfica*

- **Qué incluir:** Precisar si la política aplica a todas las sedes o a ubicaciones específicas.
- **Cómo especificarlo:** Declarar explícitamente las áreas geográficas, por ejemplo:
    - Todas las oficinas de la CAS (oficina principal y 5 sedes).
    - Acceso remoto a través de conexiones seguras desde ubicaciones autorizadas.
    - Operaciones en municipios bajo la jurisdicción de la CAS.

2.1.1.4 *Procesos y Servicios Cubiertos*

- **Qué incluir:** Identificar los procesos o servicios específicos que requieren protección bajo la política.
- **Cómo especificarlo:** Listar los procesos críticos, por ejemplo:
    - Gestión de solicitudes ciudadanas en la sede electrónica.
    - Control de recursos ambientales y seguimiento de licencias.
    - Gestión de datos personales conforme a la Ley 1581 de 2012.
    - Administración de sistemas de información y plataformas digitales.

2.1.1.5 *Exclusiones del Alcance*

- **Qué incluir:** Especificar lo que **no** está cubierto por la política.
- **Cómo especificarlo:** Indicar los sistemas, procesos o activos fuera del alcance, por ejemplo:
    - Equipos personales no conectados a la red institucional.

- Sistemas o bases de datos históricas que no se utilicen activamente.

2.1.1.6 Acceso y Responsabilidades

- **Qué incluir:** Definir claramente quién puede acceder a los activos y bajo qué condiciones.
- **Cómo especificarlo:** Ejemplos de límites específicos:
  - Acceso a la información clasificada exclusivamente por personal autorizado.
  - Contratistas solo tendrán acceso a sistemas mediante acuerdos de confidencialidad.
  - Se requiere autenticación de múltiples factores para acceder a bases de datos críticas.

2.1.1.7 Periodicidad del Alcance

- **Qué incluir:** Determinar si el alcance se revisará y actualizará regularmente.
- **Cómo especificarlo:** Establecer plazos claros, como:
  - Revisión anual del alcance para incluir nuevos activos, riesgos o procesos.
  - Modificación en caso de implementación de nuevos sistemas.

2.1.2 Declaración de Alcance

"Esta política de seguridad de la información aplica a todos los activos digitales y físicos que almacenen, procesen o transmitan información ambiental de la CAS, incluyendo sistemas críticos como el portal de la sede electrónica, el sistema de gestión de licencias ambientales, el sistema de información financiero y contable, y las bases de datos de usuarios. Cubre a todos los funcionarios, contratistas y proveedores que interactúan con estos sistemas, tanto de forma presencial en las oficinas principales como mediante acceso remoto seguro. Se excluyen dispositivos personales no gestionados por la entidad. La política será revisada anualmente y ajustada según nuevas necesidades operativas o riesgos identificados."

2.2 Identificación de Riesgos de la Entidad según la política de Seguridad de la información.

El manual menciona la importancia de la **gestión de riesgos** de seguridad de la información y define conceptos relacionados, como:

- **Análisis de riesgos:** Identificación y evaluación de amenazas y vulnerabilidades.
- **Evaluación del riesgo:** Valoración del impacto y la probabilidad de materialización de riesgos.
- **Gestión del riesgo:** Implementación de medidas de control para mitigar los riesgos identificados.

Sin embargo, el documento no detalla los riesgos específicos identificados para la entidad ni presenta un inventario de amenazas o vulnerabilidades. Tampoco se describe el proceso utilizado para realizar la evaluación de riesgos.

Recomendación:

Incorporar una sección específica donde se liste y describa claramente los riesgos relevantes para la entidad, alineados con su operación ambiental, como amenazas de ciberseguridad, incumplimientos normativos, o riesgos operacionales.

2.2.1 Identificación y clasificación de riesgos.

La identificación de riesgos debe basarse en un análisis detallado de las actividades, procesos y activos de información. Estos son algunos riesgos comunes que podrían ser considerados por el área de tecnología, más exactamente por el Oficial de Seguridad de la CAS.

Riesgos Tecnológicos:

- **Ciberataques:** Phishing, ransomware, denegación de servicio (DDoS).
- **Pérdida de datos:** Borrado accidental, daño físico a servidores, o fallos de sistemas de respaldo.
- **Acceso no autorizado:** Credenciales robadas, configuraciones débiles, o fallas en los controles de acceso.
- **Vulnerabilidades en software:** Explotación de aplicaciones no actualizadas o mal configuradas.
- **Interrupciones de servicio:** Fallos en la infraestructura de TI (servidores, red, energía).

Riesgos Humanos:

- **Errores operativos:** Configuración incorrecta de sistemas o pérdida accidental de datos.
- **Desconocimiento:** Falta de capacitación en seguridad para empleados.
- **Fugas de información:** Uso indebido o robo de datos por parte de empleados o terceros.
- **Amenazas internas:** Acciones malintencionadas de empleados descontentos.

Riesgos Legales y Regulatorios:

- **Incumplimiento normativo:** Sanciones por no cumplir con la Ley 1581 de 2012 (Protección de Datos Personales).
- **Fallas en contratos:** Términos insuficientes con proveedores relacionados con la seguridad.

Riesgos Operativos:

- **Procesos ineficientes:** Controles manuales propensos a errores.
- **Dependencia de terceros:** Fallos en servicios externos como proveedores de nube o internet.

Este documento tiene como anexo, la identificación de los 93 riesgos clasificados en cuatro categorías según ISO/IEC 27001, el cual debe ser revisado para aplicar en la matriz de riesgos los que deba gestionar la CAS Santander y que puedan afectar su operación, o amenazar la continuidad del negocio. Ver Anexo al final del documento.

2.2.2 Clasificación de Riesgos

Una vez identificados, los riesgos deben clasificarse según su **impacto** y **probabilidad**. La siguiente matriz presenta un ejemplo de clasificación en impacto en la entidad que deben ser nuevamente identificados según lo que aplique para la CAS Santander.

Riesgo	**Probabilidad**	**Impacto**	**Nivel de Riesgo**
Ciberataque (Phishing)	Alta	Alto	Crítico
Pérdida de datos	Media	Alto	Alto
Fugas de información	Baja	Alto	Moderado
Fallo en sistemas de respaldo	Media	Medio	Moderado

2.2.3 Relacionar Riesgos con Controles

Para cada riesgo, es necesario definir los controles necesarios para gestionarlo. Esto puede incluir medidas preventivas, detectivas y correctivas, por ejemplo:

Riesgo	**Control Implementado**
Ciberataque (Phishing)	Capacitación en reconocimiento de correos maliciosos; MFA habilitado.
Pérdida de datos	Backups automáticos y verificados; pruebas de recuperación de datos.
Acceso no autorizado	Políticas de contraseñas fuertes; revisiones periódicas de accesos.
Fugas de información	Implementación de DLP (Prevención de Pérdidas de Datos).

2.2.4 Tareas, Incorporar la Lista en el Documento de la política para su gestión

La actual política de seguridad y privacidad de la información, debe incorporar las recomendaciones que se han establecido en este capítulo, es muy importante establecer una mesa de trabajo que permita a la entidad dejar explícitamente dicho el foco de la gestión de riesgos, identificarlos, clasificarlos y establecer los controles para cada uno de estos, documentar y comunicar a la entidad como se dará el tratamiento de los mismos, e igualmente en caso de materializarse alguno de los riesgos tener definido un procedimiento para su mitigación y/o minimización y garantizar la continuidad de los procesos.

Por ejemplo, el foco de la gestión de riesgos:

"La gestión de riesgos de la seguridad de la información de la CAS incluye los siguientes riesgos identificados como críticos para los activos y procesos institucionales. Cada uno de estos riesgos se encuentra sujeto a evaluaciones periódicas y cuenta con controles establecidos para su mitigación, incluyendo medidas técnicas, administrativas y legales. Entre los principales riesgos se encuentran:"

- Ciberataques (Phishing, ransomware, etc.).
- Pérdida de datos por fallas técnicas o errores humanos.
- Acceso no autorizado a sistemas críticos.
- Incumplimiento de normativas legales sobre protección de datos personales.
- Interrupciones en los servicios tecnológicos críticos.

"Esta lista será revisada y actualizada anualmente como parte del proceso de mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI)."

Igualmente, el documento de Política de Seguridad y privacidad de la información se debe realizar la respectiva documentación y socialización.

- **Documentar:** Incluir la lista de riesgos en el **Análisis de Riesgos del SGSI** y vincularla con políticas y procedimientos específicos.
- **Comunicar:** Asegurar que los responsables de los controles y los equipos operativos comprendan los riesgos relevantes y cómo manejarlos.

De esta forma, la política de seguridad no solo refleja un compromiso general, sino que también detalla las amenazas concretas que se gestionan en la entidad.

2.3 Desarrollo de Políticas y Objetivos de Seguridad

El manual incluye una declaración de política general de seguridad de la información, donde la Dirección General de la CAS se compromete a:

- Preservar la confidencialidad, integridad y disponibilidad de los activos de información.
- Garantizar el cumplimiento de la legislación vigente, como la Ley 1581 de 2012 (Protección de Datos Personales).
- Fortalecer la cultura de seguridad entre los funcionarios, contratistas y terceros.

Se establecen los siguientes **objetivos de seguridad**:

- Proteger los activos de información frente a accesos no autorizados, alteraciones y pérdidas.
- Implementar controles técnicos, administrativos y físicos para mitigar riesgos.
- Fomentar una mejora continua en los procesos de seguridad de la información.
- *Mantener un sistema de gestión alineado con las normas internacionales, como ISO/IEC 27001.*

El documento también menciona que las políticas serán revisadas periódicamente y ajustadas según sea necesario.

Recomendaciones:

Para dar cumplimiento a la declaración de política y a sus objetivos estratégicos de seguridad, la actual administración de la CAS Santander, debe apoyar la implementación de los lineamientos de seguridad de la información establecidos en las buenas prácticas de la norma ISO/IEC 27001, para buscar avanzar hacia un modelo de gestión formal que vaya madurando de manera incremental bajo un modelo de mejora continua.

Este apoyo será evidente con las siguientes acciones específicas:

- Adopción de la nueva política, debidamente ajustada y actualizada
- Asignación de un oficial de Seguridad para la entidad
- Aprobación de un plan para el tratamiento de riesgos con su debido presupuesto.

Una vez ajustado el documento que obra como un marco de comportamiento que debe seguir la CAS para cumplir los objetivos de un MSPI, es necesario avanzar ya en un plan que permita pasar a la acción y para ello a partir de estas líneas se presentará la estrategia para materializar el marco definido en el MSPI, para ir en concreto a la implementación de un Sistema de Gestión para la Seguridad de la información, SGSI.

3 Análisis del Estado Actual de la Seguridad de la Información, diagnóstico.

Para iniciar la implementación del SGSI, es fundamental realizar un diagnóstico que evalúe el estado actual de la entidad en términos de seguridad de la información. Este diagnóstico permite identificar brechas y áreas de mejora, que debe incluir aspectos como el nivel de madurez del sistema de seguridad, identificación de amenazas y vulnerabilidades, y la existencia de políticas y procedimientos relacionados con la seguridad de la información.

El primer paso es hacer una medición de cumplimiento o de madurez que evalué la gestión de seguridad de la información, dicha evaluación permitirá a la entidad clasificarse en una de las siguientes categorías:

- **Inicial (Ad hoc):** No existe una gestión formal de la seguridad de la información. Las acciones son reactivas.
- **Repetible:** Se aplican medidas de seguridad, pero no están documentadas ni estandarizadas.
- **Definido:** Existen políticas, procesos y estándares documentados y en uso.
- **Gestionado:** La gestión de seguridad está monitoreada y se evalúa regularmente.
- **Optimizado:** Mejora continua, basada en métricas y análisis de tendencias.

Matriz de Evaluación del Nivel de Madurez del SGSI.

Esta matriz permite evaluar el nivel de madurez de una entidad en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI). Cada dimensión incluye preguntas clave que deben ser calificadas en una escala de 1 a 5, donde:

1 = No implementado, 2 = Implementado parcialmente, 3 = Implementado, 4 = Gestionado, 5 = Optimizado.

Dimensión	Pregunta	Calificación (1-5)
Políticas y procedimientos	¿La entidad tiene una política de seguridad de la información aprobada y vigente?	3
	¿Existen procedimientos para gestionar incidentes de seguridad?	1
	¿Los empleados conocen y aplican las políticas de seguridad?	2
Gestión de riesgos	¿Se realizan análisis de riesgos regularmente?	1
	¿Se han identificado activos críticos y evaluado sus vulnerabilidades?	1
	¿Se asignan responsables para la mitigación de riesgos identificados?	2
Controles tecnológicos	¿Existen medidas de protección contra accesos no autorizados (como firewalls, autenticación multifactor)?	3
	¿Se realizan copias de seguridad regularmente?	3
	¿Se gestionan actualizaciones de software y hardware para evitar vulnerabilidades?	3
Gestión de incidentes	¿Existen procedimientos documentados para gestionar incidentes de seguridad?	1
	¿Se llevan registros de los incidentes y se analizan para mejorar?	1
Monitoreo y auditorías	¿Se realizan auditorías internas para verificar el cumplimiento de la política de seguridad?	1
	¿Se supervisan los sistemas en tiempo real para detectar posibles amenazas?	1

Una vez respondida la matriz, se realiza la calificación, que puede estar bajo las siguientes métricas:

- **0-20%**: Nivel inicial.
- **21-40%**: Nivel repetible.
- **41-60%**: Nivel definido.
- **61-80%**: Nivel gestionado.
- **81-100%**: Nivel optimizado.

Si aplicamos el diagnóstico con un mayor nivel de detalle y con base en ISO/27001, tendríamos una matriz así:

Esta matriz incluye un nivel de detalle ampliado para evaluar los controles tecnológicos alineados con la ISO 27001, asociando cada control a indicadores clave de desempeño (KPI). Cada control se evalúa en una escala de 1 a 5, donde: 1 = No implementado, 2 = Implementado parcialmente, 3 = Implementado, 4 = Gestionado, 5 = Optimizado. Se proporciona un espacio para observaciones y recomendaciones por cada control.

Dominio	Control Detallado	Indicador (KPI)	Calificación (1-5)	Observaciones / Recomendaciones
Control de Acceso	¿Existen políticas documentadas que regulen el acceso basado en roles (RBAC)?	Porcentaje de cuentas configuradas con roles específicos.	1	
	¿Las cuentas inactivas son deshabilitadas después de un período específico?	Tiempo promedio para deshabilitar cuentas inactivas.	2	
	¿Existen procedimientos para la revocación de accesos cuando un empleado cambia de rol o deja la organización?	Porcentaje de cuentas revocadas dentro del tiempo estipulado (por ejemplo, 24 horas).	1	
	¿Se requiere autenticación multifactor (MFA) para todos los accesos a sistemas críticos?	Porcentaje de sistemas críticos que utilizan MFA.	1	
	¿Se utilizan estándares de contraseñas (longitud mínima, complejidad, expiración)?	Porcentaje de usuarios con contraseñas que cumplen los estándares definidos.	1	
Gestión de Activos	¿El inventario incluye información sobre propietarios de activos?	Porcentaje de activos con propietarios definidos en el inventario.	1	
	¿Se realiza una auditoría periódica para verificar la actualización del inventario?	Frecuencia de auditorías del inventario (mensual, trimestral, anual).	1	
	¿Están clasificados los activos de acuerdo con su nivel de	Porcentaje de activos clasificados según	2	

	criticidad y sensibilidad?	criticidad y sensibilidad.		
	¿Se aplican controles físicos para proteger activos críticos?	Número de incidentes reportados relacionados con activos críticos por falta de controles físicos.	1	
	¿Se documentan los procedimientos para la eliminación segura de activos en desuso?	Porcentaje de activos eliminados siguiendo los procedimientos documentados.	1	
Protección contra Malware	¿Los sistemas antivirus/antimalware se encuentran configurados para actualizaciones automáticas?	Porcentaje de sistemas con actualizaciones automáticas activadas.	3	
	¿Se monitorean las actividades sospechosas en tiempo real?	Número de alertas procesadas y gestionadas por mes.	2	
	¿Se restringe la instalación de software no autorizado en dispositivos corporativos?	Porcentaje de dispositivos con políticas de restricción de software aplicadas.	1	
	¿Se realizan campañas periódicas para concientizar sobre amenazas como ransomware y phishing?	Número de campañas realizadas por año.	2	
	¿Se evalúa la efectividad de las capacitaciones mediante simulaciones de ataques?	Tasa de éxito en simulaciones de ataques (porcentaje de usuarios que detectan el ataque).	1	
Copia de Seguridad	¿Las copias de seguridad son cifradas para proteger la confidencialidad de los datos?	Porcentaje de copias de seguridad cifradas.	1	
	¿Se documentan los procedimientos para la creación, almacenamiento y	Porcentaje de procedimientos documentados y validados.	1	

	restauración de las copias?			
	¿Se realizan pruebas de recuperación al menos una vez al trimestre?	Frecuencia de pruebas de recuperación exitosas.	1	
	¿Se almacenan copias en diferentes ubicaciones físicas para proteger contra desastres?	Porcentaje de copias almacenadas en ubicaciones separadas.	1	
	¿Se aplican controles de acceso físico y lógico a los sistemas de almacenamiento?	Número de incidentes de acceso no autorizado a sistemas de almacenamiento.	1	
Gestión de Incidentes	¿Existe un equipo de respuesta a incidentes (CSIRT) formalmente definido?	Número de incidentes gestionados por el CSIRT por mes.	1	
	¿Los incidentes se documentan y clasifican según su impacto?	Porcentaje de incidentes documentados y clasificados.	3	
	¿Se comunican los incidentes relevantes a las partes interesadas internas y externas?	Tiempo promedio para comunicar incidentes relevantes.	2	
	¿Se realizan análisis post-incidente para identificar las causas raíz?	Porcentaje de incidentes con análisis post-incidente completado.	2	
	¿Se revisa y actualiza el plan de respuesta a incidentes con base en lecciones aprendidas?	Frecuencia de actualizaciones al plan de respuesta a incidentes.	1	

Al evaluar las anteriores matrices se pudo evidenciar que la *CAS Santander, tiene un nivel de madurez Inicial*, lo que implica desarrollar con carácter urgente un plan de trabajo para el corto y mediano plazo que permita avanzar en la implementación de buenas prácticas basadas en ISO/27001, que cumple con lo definido por el modelo MSPI.

La CAS Santander, igualmente tiene establecido en su PETI 2025-2027, un proyecto relacionado con el Tratamiento de Datos Personales, que esta alineado a lo definido en el MSPI, si bien Tratamiento de Datos Personales está definido en uno de los dominios del MSPI, es una buena iniciativa para empezar a dar cumplimiento a la normatividad.

A continuación, se presenta un cuadro que establece el alcance de lo que es Tratamiento de datos personales y MSPI, para mayor ilustración.

Área/Concepto	**Protección de Datos**	**MSPI (Modelo de Seguridad y Privacidad de la Información)**
Enfoque Principal	Protección de los **datos personales** de los individuos.	Protección de **toda la información** de la entidad, incluyendo datos personales, financieros, operativos, etc.
Normatividad Principal	Ley 1581 de 2012 y Decreto 1377 de 2013.	Estándares internacionales como ISO 27001, normas locales de ciberseguridad, NIST, y directrices específicas de seguridad.
Cobertura de Información	Solo datos personales (nombres, direcciones, correos, etc.).	Toda la información manejada por la entidad: datos personales, información confidencial, datos financieros, operativos, etc.
Objetivo General	Garantizar los derechos de los titulares sobre sus datos personales y evitar el uso no autorizado o indebido de esos datos.	Asegurar la **confidencialidad, integridad y disponibilidad** de toda la información de la entidad, incluyendo la protección frente a amenazas internas y externas.
Gestión de Riesgos	Identificación y mitigación de riesgos asociados a la recolección, almacenamiento y tratamiento de datos personales.	Gestión de riesgos amplia: amenazas informáticas, físicas, operativas, incidentes de ciberseguridad, etc., que puedan comprometer cualquier tipo de información.
Medidas Técnicas y Administrativas	Controles específicos para proteger datos personales (encriptación, consentimiento, control de acceso a datos personales).	Medidas integrales que incluyen políticas de seguridad, gestión de accesos, protección física, políticas de backup, monitoreo y respuesta a incidentes para toda la infraestructura de la información.
Derechos del Titular	Enfoque en asegurar que los titulares puedan ejercer sus derechos (acceso, rectificación, supresión, etc.).	No aplica directamente, pero incluye medidas para garantizar que la información esté protegida y accesible solo por personas autorizadas.
Notificación de Incidentes	Obligación de notificar a la Superintendencia de Industria y Comercio (SIC) y a los titulares en caso de violación de datos personales.	Gestión y notificación de **incidentes de seguridad** en toda la información de la organización, con planes de respuesta a incidentes y protocolos de actuación (aunque no siempre requiere notificación pública, depende de la normativa).
Auditoría y Monitoreo	Auditorías para asegurar el cumplimiento de las políticas de protección de datos personales.	Auditorías de seguridad más amplias, que cubren el sistema completo de gestión de seguridad de la información, basadas en marcos normativos como ISO 27001.
Capacitación	Capacitación del personal en manejo y protección de datos personales.	Capacitación en **seguridad de la información** para todo el personal, abarcando no solo datos personales, sino también otros aspectos como ciberseguridad y manejo seguro de información confidencial.
Tecnologías Involucradas	Herramientas para garantizar la protección de datos personales (encriptación, sistemas de control de acceso a datos).	Soluciones integrales de seguridad: firewalls, SIEM (Security Information and Event Management), detección de intrusos, criptografía, autenticación multifactor, etc.

Área/Concepto	Protección de Datos	MSPI (Modelo de Seguridad y Privacidad de la Información)
Revisión y Actualización	Revisión periódica de la política de tratamiento de datos y medidas para la protección de datos personales.	Ciclo continuo de mejora y actualización del **sistema de gestión de seguridad de la información**, incluyendo la respuesta a nuevas amenazas y vulnerabilidades.

3.1 Revisión del Cumplimiento Normativo:

Verificar el cumplimiento con normativas nacionales, como la Ley 1581 de 2012 sobre protección de datos personales y el Decreto 1078 de 2015 que regula las TIC.

Esta matriz permite evaluar y evidenciar el cumplimiento de los requisitos normativos establecidos en la Ley 1581 de 2012 y el Decreto 1078 de 2015. Cada criterio se evalúa en una escala de 1 a 5, donde: 1 = No implementado, 2 = Implementado parcialmente, 3 = Implementado, 4 = Gestionado, 5 = Optimizado. Se proporciona un espacio para observaciones y recomendaciones.

Normativa	Requisito	Indicador (KPI)	Calificación (1-5)	Observaciones / Evidencias
Ley 1581 de 2012	Inventario de bases de datos actualizado	Porcentaje de bases de datos inventariadas.	2	
Ley 1581 de 2012	Inscripción en el RNBD	Porcentaje de bases de datos inscritas en el RNBD.	2	
Ley 1581 de 2012	Política de tratamiento de datos aprobada y publicada	Disponibilidad de la política en medios institucionales.	2	
Ley 1581 de 2012	Mecanismos de consentimiento informado implementados	Porcentaje de datos recolectados con consentimiento verificable.	2	
Ley 1581 de 2012	Procedimientos para atender derechos de los titulares	Tiempo promedio de respuesta a solicitudes de titulares.	2	
Ley 1581 de 2012	Capacitaciones realizadas en protección de datos	Porcentaje de empleados capacitados anualmente.	2	
Ley 1581 de 2012	Medidas técnicas y administrativas para la seguridad de datos personales	Número de incidentes relacionados con datos personales reportados y gestionados.	1	
Decreto 1078 de 2015	Plan de Gobierno Digital elaborado y publicado	Disponibilidad del plan en medios institucionales.	2	

Decreto 1078 de 2015	Servicios ciudadanos digitales implementados	Número de servicios digitales interoperables activos.	2	
Decreto 1078 de 2015	Cumplimiento de estándares de interoperabilidad	Porcentaje de sistemas compatibles con estándares de interoperabilidad.	1	
Decreto 1078 de 2015	Publicación de datos abiertos	Número de conjuntos de datos publicados en el portal de datos abiertos.	3	
Decreto 1078 de 2015	Modelo de Seguridad y Privacidad de la Información implementado	Porcentaje de controles de seguridad implementados según el MSPI.	2	
Decreto 1078 de 2015	Capacitaciones realizadas en gobierno digital	Porcentaje de empleados capacitados en herramientas digitales.	2	

Conclusión:

Se requiere formalmente avanzar hacia la implementación de un modelo de buenas prácticas como el que define ISO/IEC-27001, de tal forma que los actuales niveles de riesgo identificados en las diferentes matrices permitan llegar a un nivel de madurez GESTIONADO, esto implica los siguientes aspectos:

- Institucionalizar y ejecutar acciones según lo establecido en la política de seguridad de la información.
- Contar con una organización formal que pueda hacer la Gobernanza del sistema de Seguridad de la Información.
- Contar con un oficial de Seguridad en la CAS.
- Establecer presupuesto para garantizar la incorporación de herramientas y buenas practicas en el tratamiento de información y las fuentes generadoras de estas.
- Comprometer a todos los contratistas en el cumplimiento de las normativas y acciones requeridas por el SGSI.

4 Estructura metodológica para implementar un SGSI, Sistema de Gestión de la seguridad de la información.

Antes de desarrollar la estructura metodológica de un SGSI, es importante aclarar su diferencia con el MSPI, el objetivo para la CAS es avanzar en un SGSI, con el fin de cumplir los lineamientos o marco de referencia de un modelo de seguridad y privacidad de la información. A continuación, se establecen las diferencias:

Un MSPI (Modelo o Marco de Seguridad y Protección de la Información) y un SGSI (Sistema de Gestión de la Seguridad de la Información) no son exactamente lo mismo, aunque ambos se relacionan con la protección y gestión de la información en una organización.

En primer lugar, un MSPI suele entenderse como un conjunto de lineamientos, principios y conceptos que proporcionan una base teórica o un marco de referencia para la protección de la información. Este modelo establece las directrices generales, las áreas de atención, las dimensiones de la seguridad (confidencialidad, integridad, disponibilidad) y los objetivos estratégicos que deben alcanzarse. Sin embargo, no necesariamente implica la existencia de un ciclo de mejora continua o de un sistema formalizado para su implementación práctica. Este MSPI puede ser cumplido en buena parte con la política de seguridad.

Por otro lado, un SGSI, tal como se define comúnmente en normas internacionales como ISO/IEC 27001, es un sistema formal y estructurado que no solo establece políticas y procedimientos, sino que además incorpora procesos de evaluación de riesgos, controles específicos, auditorías internas, mejora continua y supervisión constante.

Un SGSI es más que un conjunto de lineamientos: es una metodología operativa que asegura la implementación efectiva de las medidas de seguridad, su mantenimiento en el tiempo y su adaptación ante cambios en el entorno o en las amenazas.

Entonces, mientras que un MSPI brinda un marco conceptual sobre qué proteger y por qué, el SGSI representa un sistema de gestión integral que define cómo proteger, cómo verificar la eficacia de las medidas y cómo mejorar continuamente el nivel de seguridad de la información en la organización.

Podría decirse que, en cierta medida, el SGSI es la puesta en práctica formal y sistemática de las buenas prácticas, lineamientos y principios que se presentan en un MSPI. Mientras que el MSPI ofrece el conjunto de orientaciones, objetivos y marcos conceptuales para la protección de la información, el SGSI se encarga de traducir estas directrices en un sistema estructurado y operativo.

En ese sentido, el SGSI incorpora procesos de gestión, roles claros, políticas, procedimientos, herramientas de seguimiento, auditorías internas, así como la mejora continua. Todo ello permite asegurar que las buenas prácticas propuestas por el MSPI no se queden en un plano meramente teórico, sino que se apliquen de manera tangible y controlada en el entorno organizativo.

Por lo tanto, en este documento hablaremos del plan para la implementación de un Sistema de Gestión de Seguridad de la información, SGSI, que es en última instancia el verdadero valor que se requiere implementar en la CAS Santander. Para mayor lustración a continuación se presenta un modelo a seguir para su implementación que desarrollaremos en este documento.

4.1 Esquema visual del ciclo de vida del SGSI basado en ISO27001.

La siguiente gráfica presenta las fases que un SGSI debe cumplir para su planificación, puesta en ejecución seguimiento y ajustes, si se revisa de manera estricta lo que esta imagen establece, es muy importante contar con una organización que permita su gestión y procesos de control y mejora continua. Actualmente la CAS Santander no cuenta con una organización que permita formalmente establecer el sistema, pero es importante avanzar sobre este objetivo y para ello se debe tener en cuenta la estrategia establecida en este documento que finalmente se traduce en un plan para la implementación, este plan debe avanzar por ciclos y actividades que permitan ir logrando la mayor madurez posible y sobre todo buscar desde el inicio cumplir con los objetivos estratégicos del modelo MSPI, que son, Preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos, Orientar la gestión adecuada del ciclo de vida de la seguridad de la información y Habilitar la implementación de la Política de Gobierno Digital.

Según ISO27001, este ciclo debe tener en cuenta lo siguiente:

Planificar (Plan)

- **Definir el alcance del SGSI**: Identificar límites y partes relevantes.
- **Realizar análisis de riesgos**: Identificar, evaluar y priorizar los riesgos.
- **Desarrollar políticas y objetivos de seguridad**: Asegurar la alineación con los objetivos estratégicos.
- **Seleccionar controles de seguridad**: Según el Anexo A en ISO/IEC 27001:2022, personalizados según las necesidades, esta versión cuenta con 93 controles organizados en cuatro categorías.
- **Crear el plan de tratamiento de riesgos**.

Hacer (Do)

- **Implementar los controles seleccionados**: Incorporar medidas técnicas, organizativas y físicas.
- **Capacitar al personal**: Sensibilizar sobre seguridad de la información.
- **Operar los procesos del SGSI**: Garantizar que se ejecuten las políticas y procedimientos establecidos.

Verificar (Check)

- **Monitorear y medir**: Revisar el desempeño de los controles y el SGSI.
- **Auditorías internas**: Identificar no conformidades y áreas de mejora.
- **Evaluar riesgos periódicamente**: Revisar si los riesgos han cambiado.

Actuar (Act)

- **Tomar acciones correctivas y preventivas**: Basadas en resultados de auditorías y monitoreo.
- **Actualizar el SGSI**: Incorporar mejoras según nuevas necesidades o riesgos identificados.
- **Revisar el sistema de manera periódica**: A través de la dirección.

4.2 Plan de acción para implementar un SGSI en la CAS Santander.

Plan de trabajo para la implementación de la norma ISO/IEC-27001, para corto y mediano plazo.

4.2.1 Corto plazo (0-6 meses)

Objetivo: Establecer una base mínima de controles esenciales para reducir riesgos críticos.

1. **Definición de roles y responsabilidades**:
    - Crear un Comité de Seguridad de la Información para liderar las actividades.
    - Nombrar un responsable de seguridad (ISO - Information Security Officer).
2. **Formalización de políticas básicas**:
    - Redactar y aprobar políticas mínimas:
        - Política de control de accesos.
        - Política de gestión de incidentes.
        - Política de copias de seguridad.
    - Socializar estas políticas con los empleados.
3. **Implementación de controles tecnológicos básicos**:
    - **Control de accesos**:
        - Deshabilitar cuentas inactivas y limitar accesos innecesarios.
        - Implementar autenticación multifactor (MFA) en sistemas críticos.
    - **Copia de seguridad**:
        - Realizar respaldos periódicos de datos críticos y almacenarlos en ubicaciones seguras.
        - Almacenar copias en ubicaciones seguras
    - **Protección contra malware**:
        - Instalar y configurar antivirus actualizado en todos los dispositivos.
        - Restringir la instalación de software no autorizado.
4. **Gestión básica de incidentes**:
    - Crear un procedimiento simplificado para registrar, analizar y gestionar incidentes.
    - Establecer un canal único para reportar incidentes.
5. **Capacitación inicial**:
    - Realizar talleres básicos de sensibilización sobre temas como phishing, malware y uso seguro de contraseñas.

4.2.2 Mediano plazo (6-12 meses)

Objetivo: Fortalecer los controles y avanzar hacia un nivel de gestión organizado.

1. **Estandarización de procesos**:
    - Implementar procedimientos formales basados en ISO 27001 para:
        - Gestión de activos (inventario y clasificación).
        - Gestión de riesgos (identificación, evaluación y tratamiento).
        - Gestión de accesos basados en roles (Roles-Based Access Control - RBAC).
    - Consolidar un Manual de seguridad de la información, Integrar los procesos en un manual operativo.
2. **Ampliación de controles tecnológicos**:
    - Monitoreo continuo:
        - Configurar herramientas para la detección y alerta de actividades sospechosas.
    - Mejorar copias de seguridad:
        - Implementar cifrado de datos en reposo y en tránsito.
        - Realizar pruebas regulares de recuperación.

    - Expansión de autenticación:
        - Aplicar MFA a todos los usuarios.
3. **Gestión avanzada de incidentes**:
    - Crear un equipo de respuesta a incidentes (CSIRT).
    - Realizar simulacros de incidentes para medir la efectividad del plan.
4. **Monitoreo y auditorías**:
    - Implementar auditorías internas trimestrales para verificar cumplimiento.
    - Medir los KPIs definidos en la matriz para evaluar progresos.
5. **Capacitación continua**:
    - Iniciar programas de formación más avanzados para roles clave, ISO, CSIRT, Administradores de Sistemas)
    - Realizar simulaciones de phishing para evaluar y mejorar la concienciación.

4.3 Indicadores de éxito

Para evaluar el avance del plan, se debe utilizar indicadores como:

- **Reducción del tiempo promedio de gestión de incidentes**.
- **Porcentaje de políticas implementadas y socializadas**.
- **Porcentaje de sistemas críticos con MFA implementado**.
- **Número de simulacros de incidentes realizados**.
- **Frecuencia y éxito en las pruebas de recuperación de datos**.

Este plan progresivo permitirá a la entidad CAS Santander abordar los aspectos críticos de la seguridad de la información en el corto plazo, mientras establece una base sólida para la gestión a mediano plazo. La implementación continua de controles, la capacitación del personal y la evaluación periódica garantizarán la mejora continua y la protección de los activos de información, a parir de avanzar sobre un modelo formal para reducir riesgos críticos en el corto plazo, establecer procesos organizados y medibles en el mediano plazo, crear una base sólida para alcanzar niveles avanzados en la gestión de seguridad de la información.

4.4 Gobernanza para la Seguridad de la información.

El objetivo de establecer institucionalmente una estructura para la gobernanza de la seguridad de la información según el SGSI, no es un mero cumplimiento, es una estrategia para poder involucrar a toda la organización en el cumplimiento de políticas y procedimientos que deben acatarse por parte de los diferentes estamentos de la entidad.

Igualmente es una estrategia para que la alta dirección este no solo al tanto de los requerimientos, sino que tome conciencia y pueda apoyar decididamente la protección de los diferentes activos de información, y se busque siempre la continuidad del negocio en lo que compete al área de tecnología.

Una propuesta para la gobernanza del SGSI, en la CAS Santander puede estar organizado de la siguiente forma.

4.4.1 Comité Estratégico de Seguridad y Privacidad de la Información

Objetivo: Asegurar que las decisiones de seguridad y privacidad están alineadas con los objetivos estratégicos de la entidad.

- **Integrantes**:
    - **Director General**: Responsable de aprobar políticas de alto nivel y recursos para implementar el MSPI.

    - **Oficial de Seguridad y Privacidad de la Información (CISO/CSPO)**: Presenta el estado del MSPI, riesgos identificados y propuestas de mejora.
    - **Director de Tecnología o CIO**: Garantiza la integración de la seguridad y privacidad en las iniciativas de TI.
    - **Auditor Interno**: Supervisa que se cumplan los controles y normativas aplicables.
    - **Representantes de áreas clave** (jurídica, recursos humanos, operaciones, etc.): Proveen insumos y alinean sus procesos con el MSPI.
- **Funciones**:
    - Aprobar políticas y normas.
    - Revisar informes de auditoría y cumplimiento.
    - Priorizar inversiones en seguridad y privacidad.
    - Aprobar la gestión de riesgos críticos.

4.4.2 Comité Operativo de Seguridad y Privacidad

Objetivo: Ejecutar y supervisar las acciones operativas del SGSI.

- **Integrantes**:
    - **Oficial de Seguridad y Privacidad de la Información** (Líder del Comité): Coordina las acciones del equipo operativo.
    - **Responsable de Gestión de Riesgos**: Analiza y gestiona los riesgos asociados a la información.
    - **Administrador de Infraestructura y Redes**: Implementa controles técnicos de seguridad.
    - **Responsable de Protección de Datos Personales**: Garantiza el cumplimiento de las normas sobre privacidad (como la Ley 1581 de 2012 en Colombia).
    - **Representante de Continuidad del Negocio**: Supervisa la preparación y respuesta ante incidentes.
- **Funciones**:
    - Implementar controles técnicos, administrativos y físicos.
    - Gestionar riesgos y vulnerabilidades.
    - Responder a incidentes de seguridad.
    - Mantener actualizado el inventario de activos de información.

4.4.3 Oficinas de Apoyo o Especializadas

Objetivo: Apoyar la ejecución de tareas específicas del SGSI y garantizar el cumplimiento de normativas.

- **Integrantes y roles**:
    - **Oficina de Talento Humano**:
        - Capacitación en seguridad y privacidad.
        - Gestión de cláusulas de confidencialidad y propiedad intelectual en contratos.
    - **Oficina Jurídica**:
        - Asesoría sobre cumplimiento normativo.
        - Gestión de incidentes legales relacionados con violaciones de privacidad.
    - **Proveedor de Servicios TI**:
        - Cumplir los Acuerdos de Nivel de Servicio (SLA) establecidos.
        - Proveer actualizaciones de seguridad y monitoreo.

4.4.4 Líderes de Procesos o Áreas Funcionales

Objetivo: Ser los puntos de contacto en sus áreas para la implementación del SGSI.

- **Funciones**:

- Garantizar la aplicación de políticas y procedimientos en su área.
- Reportar incidentes de seguridad y privacidad.
- Participar en evaluaciones de riesgos y auditorías.

4.4.5 Mecanismos de Trabajo

- **Reuniones periódicas**: Los comités estratégico y operativo se reúnen regularmente (por ejemplo, trimestralmente el estratégico y mensualmente el operativo).
- **Informes de gestión**: Indicadores como incidentes de seguridad, cumplimiento de políticas, y resultados de auditorías.
- **Planes de mejora continua**: Acciones derivadas de auditorías internas, cambios normativos o nuevas amenazas identificadas.

Este modelo asegura que la gobernanza del MSPI esté alineada con las necesidades estratégicas y operativas de la entidad, promoviendo una cultura de seguridad y privacidad.

ANEXO TECNICO CONTROLES POR CATEGORIA SEGÚN ISO/IEC-27001, versión 2022

Anexo A de la norma ISO/IEC 27001:2022, clasificados por las cuatro categorías introducidas en esta versión: *Controles Organizativos, Controles de Personas, Controles Físicos y Controles Tecnológicos*. Esta clasificación se corresponde con la estructura de ISO/IEC 27002:2022, de la cual ISO/IEC 27001:2022 deriva sus controles.

CONTROLES ORGANIZATIVOS (37 controles)

1. Políticas para la seguridad de la información
2. Roles y responsabilidades en seguridad de la información
3. Segregación de funciones
4. Gestión de conflictos de intereses
5. Contacto con las autoridades
6. Contacto con grupos de interés especializados
7. Inteligencia de amenazas
8. Seguridad de la información en la gestión de proyectos
9. Inventario de información y otros activos asociados
10. Uso aceptable de la información y activos asociados
11. Eliminación de la información
12. Clasificación de la información
13. Etiquetado de la información
14. Transferencia de la información
15. Control de acceso
16. Gestión de identidades
17. Información de autenticación (gestión de credenciales)
18. Derechos de acceso
19. Seguridad de la información en las relaciones con proveedores
20. Seguridad de la información en los acuerdos con proveedores
21. Gestión de la seguridad de la información en la cadena de suministro
22. Monitoreo, revisión y evaluación de servicios de terceros
23. Seguridad de la información en relaciones con organizaciones colaboradoras
24. Gestión de la seguridad de la información en entornos interconectados
25. Ciclo de vida de desarrollo seguro
26. Procesos seguros de desarrollo y soporte
27. Desarrollo externalizado
28. Datos de prueba
29. Eliminación segura o reutilización de equipos
30. Soportes físicos en tránsito
31. Liberación segura de código
32. Gestión de vulnerabilidades técnicas
33. Continuidad de la seguridad de la información
34. Redundancias
35. Registro (logging)
36. Sincronización de relojes
37. Información de eventos

CONTROLES DE PERSONAS (8 controles)

1. Verificación de antecedentes del personal
2. Responsabilidades en materia de seguridad de la información durante el empleo

3. Capacitación, concienciación y formación en seguridad de la información
4. Gestión del personal al finalizar o cambiar su relación laboral
5. Canal de denuncia (whistleblowing)
6. Responsabilidades en el trabajo remoto
7. Protección del personal en entornos hostiles
8. Viajes seguros

CONTROLES FÍSICOS (14 controles)

1. Perímetro físico seguro
2. Controles físicos de acceso
3. Protección contra amenazas físicas y ambientales
4. Áreas seguras de trabajo
5. Suministro seguro de servicios públicos
6. Ubicación y protección del equipo
7. Seguridad del cableado
8. Mantenimiento del equipo
9. Eliminación segura del equipo con información
10. Protección contra interrupciones eléctricas y fallos del sistema
11. Segregación física de la información crítica
12. Protección de activos fuera de las instalaciones
13. Medios de almacenamiento transportables seguros
14. Recepción y envío seguro de la información

CONTROLES TECNOLÓGICOS (34 controles)

1. Gestión del control de acceso lógico a sistemas e información
2. Autenticación y gestión de credenciales
3. Principio del privilegio mínimo en el acceso
4. Eliminación o deshabilitación de cuentas no necesarias
5. Restricciones sobre el software instalado por el usuario
6. Protección contra software malicioso
7. Copias de seguridad (backups) a nivel tecnológico
8. Registro de eventos y monitoreo de sistemas
9. Detección de anomalías
10. Seguridad de las redes
11. Control de acceso a redes y conexiones remotas
12. Seguridad de servicios en la nube
13. Seguridad de las comunicaciones
14. Seguridad del correo electrónico y mensajería
15. Protección de la información en tránsito
16. Protección de la información en reposo
17. Cifrado
18. Gestión de claves criptográficas
19. Integridad del software y las plataformas
20. Desarrollo seguro de software
21. Pruebas de seguridad del software
22. Gestión de la configuración segura
23. Gestión de vulnerabilidades técnicas
24. Monitoreo de la seguridad tecnológica
25. Respuesta a incidentes tecnológicos

26. Gestión de la capacidad y disponibilidad tecnológica
27. Protección contra ataques de denegación de servicio
28. Segregación lógica en entornos multiusuario
29. Seguridad en entornos virtualizados y contenedores
30. Seguridad de dispositivos móviles
31. Seguridad de Internet de las cosas (IoT)
32. Prevención de fuga de datos (DLP)
33. Control del uso indebido de servicios basados en información
34. Seguridad en sistemas de control industrial (ICS)

Anexo, Política de Control de Accesos.

A continuación, se presenta un modelo de política basado en los lineamientos de ISO 27001, de tal forma que la CAS Santander, pueda formalizar dicha política dentro del modelo de Seguridad y Privacidad de la información, MSPI, y materializarla en el sistema de gestión de seguridad de la información. Es recomendable que cada numeral que implica acción ir avanzando paso a paso en su implementación. Debe estar coordinada y gestionada por el Oficial de Seguridad que defina la CAS Santander.

1. Propósito

El objetivo de esta política es establecer los lineamientos necesarios para gestionar y controlar el acceso a los sistemas de información, recursos tecnológicos, y datos sensibles de la entidad, asegurando la protección de la confidencialidad, integridad y disponibilidad de la información, conforme a los requisitos de la norma ISO 27001 y la legislación aplicable.

2. Alcance

Esta política aplica a:

- Todos los empleados, contratistas, proveedores y terceros (comunidad) que accedan a los sistemas de información y recursos tecnológicos de la entidad.
- Todos los sistemas de información, bases de datos, aplicaciones, equipos, redes y otros activos tecnológicos.

3. Principios

1. **Acceso basado en necesidad y rol (Least Privilege):** El acceso a la información y sistemas estará restringido a las personas autorizadas en función de sus responsabilidades laborales y solo al nivel mínimo requerido.
2. **Autenticación robusta:** Todos los accesos deberán estar protegidos mediante métodos de autenticación seguros, como contraseñas fuertes o autenticación multifactor (MFA).
3. **Revisión periódica:** Los permisos y roles serán revisados periódicamente para asegurar que continúen siendo necesarios y apropiados.
4. **Registros de auditoría:** Todas las actividades de acceso serán registradas y monitoreadas para identificar posibles accesos no autorizados o actividades sospechosas.

4. Directrices

4.1. Gestión de Cuentas de Usuario

1. Todas las cuentas de usuario deberán ser creadas, modificadas o eliminadas exclusivamente por el área de TI mediante una solicitud documentada y aprobada.
2. Las cuentas de usuario deben estar asociadas a un individuo específico. No se permite el uso de cuentas genéricas o compartidas, salvo que sea estrictamente necesario y aprobado.
3. Las contraseñas deberán cumplir con los siguientes requisitos:
    - Longitud mínima de 12 caracteres.
    - Inclusión de letras mayúsculas, minúsculas, números y caracteres especiales.

- Cambio obligatorio cada 90 días.
- Prohibición de reutilizar las últimas 5 contraseñas.

4.2. Autenticación Multifactor (MFA)

1. El uso de MFA es obligatorio para:
   - Acceso a sistemas críticos.
   - Acceso remoto a la red corporativa.
2. Los métodos aceptables de MFA incluyen:
   - Aplicaciones de autenticación (Google Authenticator, Microsoft Authenticator).
   - Tokens físicos o virtuales.
   - Biometría.

4.3. Control de Accesos Físicos

1. El acceso a áreas restringidas, como los centros de datos, estará limitado a personal autorizado.
2. Se implementarán controles físicos como cerraduras electrónicas, tarjetas de acceso y registro de visitantes.
3. Todo acceso a áreas restringidas deberá ser registrado y auditado periódicamente.

4.4. Revisión de Accesos

1. Los permisos de acceso serán revisados trimestralmente por los responsables de área y el área de TI.
2. El acceso de empleados que cambien de rol o dejen la organización deberá ser revocado dentro de las 24 horas siguientes al cambio.
3. Las cuentas inactivas por más de 30 días serán deshabilitadas automáticamente.

4.5. Monitoreo y Registro de Accesos

1. Todas las actividades de acceso deberán ser registradas mediante herramientas de monitoreo.
2. Los registros incluirán:
   - Fecha, hora y ubicación del acceso.
   - Identidad del usuario.
   - Recursos accedidos.

   Los registros serán revisados mensualmente para identificar patrones sospechosos.

5. Roles y Responsabilidades

1. **Área de TI:**
   - Implementar y gestionar los controles definidos en esta política.
   - Revisar periódicamente los permisos de acceso.
   - Responder a incidentes relacionados con accesos no autorizados.

2. **Responsables de área:**

    - Autorizar y validar los accesos solicitados por sus colaboradores.
    - Informar cambios en el personal que requieran ajustes en los permisos.

3. **Usuarios finales:**

    - Respetar las políticas de acceso.
    - Reportar incidentes de seguridad relacionados con accesos.

6. Auditoría y Cumplimiento

1. Esta política será revisada anualmente para garantizar su vigencia y alineación con los objetivos de la organización.
2. El cumplimiento de esta política será auditado trimestralmente por el área de TI y el comité de seguridad.
3. Las violaciones a esta política podrán resultar en sanciones disciplinarias según las normativas de la organización.

7. Vigencia

Esta política entra en vigor a partir de su aprobación y será de obligatorio cumplimiento para todos los involucrados.

Aprobado por:

[Nombre y Cargo]
[Fecha]

Anexo, política de control de incidentes.

La gestión de la política de "Control de incidentes" relacionado con el MSPI debe implementarse en proceso y procedimientos formales que en lo posible cuenten con una herramienta informática que facilite su gestión y trazabilidad. En el PETI 2025-2027, se identifica un proyecto que busca a través de la intranet establecer los flujos de trabajo que permitan el registro y la debida gestión. A continuación, se presenta un modelo de política a implementar.

1. Propósito

Esta política establece los lineamientos para la identificación, registro, investigación, gestión y resolución de incidentes de seguridad de la información en la entidad. Su objetivo es minimizar el impacto de los incidentes en las operaciones, proteger los activos de información y garantizar la mejora continua en la gestión de la seguridad.

2. Alcance

Esta política aplica a:

- Todos los empleados, contratistas y terceros que accedan a los sistemas de información de la entidad.
- Todos los sistemas, aplicaciones, redes y activos tecnológicos.
- Cualquier incidente relacionado con la confidencialidad, integridad, disponibilidad o privacidad de la información.

3. Definiciones

- **Incidente de Seguridad:** Evento o serie de eventos inesperados que comprometen o pueden comprometer la seguridad de la información.
- **Evento de Seguridad:** Cualquier acción que puede ser relevante para la seguridad pero que no necesariamente representa un incidente.
- **CSIRT:** Equipo de Respuesta a Incidentes de Seguridad Informática, responsable de gestionar los incidentes.

4. Principios

1. **Detección temprana:** Los incidentes deben ser identificados lo más pronto posible para reducir su impacto.
2. **Registro y trazabilidad:** Todos los incidentes deben ser documentados de forma completa y precisa.
3. **Respuesta coordinada:** Los incidentes deben ser gestionados de manera estructurada y con roles definidos.
4. **Mejora continua:** Los aprendizajes derivados de los incidentes deben ser utilizados para fortalecer los controles de seguridad.

5. Directrices

5.1. Notificación de Incidentes

1. Todos los usuarios deben reportar incidentes de seguridad tan pronto como sean detectados utilizando los canales definidos por la entidad (correo electrónico, teléfono o portal de reportes).
2. Los incidentes críticos deben ser escalados inmediatamente al CSIRT.

5.2. Clasificación de Incidentes

Los incidentes se clasificarán según:

- **Impacto:** Bajo, medio, alto.
- **Urgencia:** Inmediata, prioritaria, normal.

5.3. Respuesta a Incidentes

1. El CSIRT (Computer Security Incident Response Team, equipo encargado de gestionar los incidentes de seguridad de la información) iniciará una investigación para determinar:
    - La causa del incidente.
    - Los sistemas o datos afectados.
    - Las medidas correctivas necesarias.
2. Dependiendo de la severidad, se activará el plan de contingencia o de recuperación.
3. Las acciones inmediatas incluirán:
    - Contención del incidente para evitar mayores daños.
    - Eliminación de las causas del incidente.
    - Restauración de los servicios afectados.

5.4. Registro y Documentación

1. Todos los incidentes deben ser registrados en un sistema de gestión de incidentes, incluyendo:
    - Fecha y hora del incidente.
    - Descripción del incidente.
    - Acciones realizadas y resultados.
2. El registro debe incluir evidencias relevantes (logs, capturas de pantalla, archivos afectados).

5.5. Análisis Post-Incidente

1. Una vez resuelto el incidente, se realizará un análisis para:
    - Identificar la causa raíz.
    - Proponer mejoras para evitar incidentes similares.
    - Evaluar la efectividad de la respuesta.
2. Se documentará un informe post-incidente que será revisado por el Comité de Seguridad de la Información.

5.6. Comunicación de Incidentes

1. Los incidentes relevantes serán comunicados a las partes interesadas internas y externas según corresponda.

2. En caso de incidentes graves que afecten datos personales, se notificará a la Superintendencia de Industria y Comercio en los términos establecidos por la ley.

5. Roles y Responsabilidades

1. **Usuarios finales:**
   - Reportar cualquier incidente de seguridad detectado.
2. **CSIRT:**
   - Gestionar los incidentes de seguridad según los procedimientos establecidos.
   - Proveer informes de incidentes a la dirección y partes interesadas.
3. **Área de TI:**
   - Implementar controles preventivos y correctivos derivados de los incidentes.
4. **Comité de Seguridad de la Información:**
   - Revisar los informes post-incidente y recomendar mejoras.

6. Auditoría y Cumplimiento

1. Esta política será revisada anualmente para garantizar su alineación con los objetivos organizacionales.
2. El cumplimiento de esta política será auditado trimestralmente.
3. Las desviaciones o incumplimientos serán reportados y tratados mediante acciones correctivas.

Vigencia

Esta política entra en vigor a partir de su aprobación y es de cumplimiento obligatorio para todos los involucrados.

Aprobado por:

[Nombre y Cargo]

[Fecha]

Anexo, Política para la Gestión de Copias de Seguridad

1. Propósito

El objetivo de esta política es establecer un marco para la creación, almacenamiento, protección y recuperación de copias de seguridad de la información crítica de la entidad. Esta política garantiza la continuidad de las operaciones en caso de pérdida de datos, desastres, o fallos en los sistemas de información, alineándose con los requisitos de la norma ISO 27001.

2. Alcance

Esta política aplica a:

- Toda la información crítica almacenada en sistemas, bases de datos y dispositivos de la entidad.
- Los empleados, contratistas y terceros responsables de la gestión y mantenimiento de sistemas de información.
- Todos los sistemas y medios utilizados para realizar copias de seguridad.

3. Principios

1. **Confidencialidad:** Las copias de seguridad deben protegerse contra accesos no autorizados.
2. **Integridad:** Garantizar que las copias de seguridad sean fidedignas y libres de corrupción.
3. **Disponibilidad:** Asegurar que las copias de seguridad estén disponibles para su restauración en caso necesario.
4. **Periodicidad:** Establecer un calendario regular para la realización de copias de seguridad.

4. Directrices

4.1. Identificación de Información Crítica

1. La información crítica será identificada y clasificada por cada área de la entidad en coordinación con el área de TI.
2. Los sistemas, aplicaciones y bases de datos que contengan información crítica deberán estar documentados.

4.2. Creación de Copias de Seguridad

1. Las copias de seguridad deberán realizarse según el siguiente calendario:
    - **Diarias:** Para datos críticos y transaccionales.
    - **Semanales:** Para configuraciones y datos secundarios.
    - **Mensuales:** Para datos de archivo y respaldo a largo plazo.
2. Las copias de seguridad deben incluir:
    - Datos críticos.
    - Configuraciones de sistemas.
    - Registros de auditoría relevantes.
3. Se debe validar la completitud y exactitud de cada copia mediante verificaciones automáticas y manuales.

4.3. Almacenamiento de Copias de Seguridad

1. Las copias de seguridad se almacenarán en:
    - Ubicaciones locales seguras (on-premise).
    - Ubicaciones remotas o en la nube para redundancia.
2. Todas las copias deben ser cifradas utilizando algoritmos robustos (AES-256 o superior).
3. Se implementará un control de acceso estricto para el almacenamiento de las copias de seguridad.
4. Las copias de seguridad se conservarán según el siguiente esquema:
    - **Diarias:** 7 días.
    - **Semanales:** 1 mes.
    - **Mensuales:** 1 año o según normativas aplicables.

4.4. Pruebas de Restauración

1. Las pruebas de restauración se realizarán:
    - Al menos trimestralmente para garantizar la efectividad de las copias.
    - Siempre que se introduzcan cambios significativos en los sistemas.
2. Todas las pruebas deberán documentarse, incluyendo resultados y acciones correctivas.

4.5. Monitoreo y Registro

1. Todas las actividades relacionadas con las copias de seguridad serán registradas en un sistema de gestión.
2. Los registros incluirán:
    - Fecha y hora de la copia.
    - Datos respaldados.
    - Responsable de la operación.
    - Resultado de la operación (exitoso o fallido).

5. Roles y Responsabilidades

1. **Área de TI:**
    - Configurar y supervisar las copias de seguridad.
    - Realizar pruebas periódicas de restauración.
    - Gestionar el almacenamiento y seguridad de las copias.
2. **Responsables de área:**
    - Identificar y comunicar información crítica.
    - Coordinar con el área de TI para asegurar el cumplimiento de esta política.
3. **Usuarios finales:**
    - Reportar datos que requieran respaldo inmediato.

6. Auditoría y Cumplimiento

1. Esta política será revisada anualmente para garantizar su vigencia.
2. Las auditorías periódicas validarán el cumplimiento de:
    - Calendarios de copia.
    - Pruebas de restauración.
    - Cifrado y almacenamiento seguro.
3. Las desviaciones serán reportadas al Comité de Seguridad de la Información.

7. Vigencia

Esta política entra en vigor a partir de su aprobación y es de cumplimiento obligatorio para todos los involucrados.

Aprobado por:

[Nombre y Cargo]

[Fecha]