COLOMBIA POTENCIA DE LA VIDA

Supersolidaria
Superintendencia de la Economía Solidaria

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024

Avenida Calle 24 (Esperanza) # 60-50 / Piso 8. Centro Empresarial Gran Estación
PBX (601) 7 560 557. Línea Gratuita 018000 180 430
www.supersolidaria.gov.co
NIT: 830.053.043-5 / Bogotá D.C., Colombia

CONTENIDO

INTRODUCCIÓN

La información se encuentra definida, como un recurso estratégico crucial para la Superintendencia de la Economía Solidaria, y es imperativo salvaguardarla de acuerdo con los principios fundamentales de legalidad, transparencia, eficiencia y seguridad. Además, se reconoce que la información constituye un derecho fundamental para los ciudadanos, quienes deben tener acceso a la misma, asegurando su confidencialidad, integridad y disponibilidad.

Con el propósito de cumplir con estas premisas, la entidad ha adoptado el Modelo de Seguridad y Privacidad de la Información (MSPI). Este modelo proporciona las herramientas necesarias para identificar, evaluar y mitigar los riesgos asociados al uso de tecnologías de la información y las comunicaciones. Asimismo, su implementación se alinea con los lineamientos establecidos en la Política de Gobierno Digital y los estándares internacionales, asegurando un enfoque integral y efectivo en la gestión de la información.

El presente documento contiene el plan de seguridad y privacidad de la información de la Super Intendencia de la Economía Solidaria, que establece los objetivos, el alcance, las responsabilidades, las actividades para mejorar la calidad y la confiabilidad de los servicios digitales de la entidad.

El plan de seguridad y privacidad de la información es un instrumento dinámico y flexible, que se actualizará periódicamente de acuerdo con los cambios en el contexto, las necesidades y las expectativas de los usuarios, y los avances tecnológicos. El plan de seguridad y privacidad de la información es un compromiso de la Superintendencia de la Economía Solidaria con la protección de la información, como un recurso clave para el desarrollo social y económico del país.

OBJETIVO

Implementar de manera efectiva las actividades definidas en el Modelo de Seguridad y Privacidad de la Información (MSPI) de la política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), alineándolas con los estándares de la NTC/IEC ISO 27001, la Política Pública de Seguridad Digital, y los criterios de Continuidad de la Operación de los servicios. Esto garantizará la seguridad y privacidad de la información en los procesos de la entidad, fortaleciendo así la gestión integral de la seguridad de la información.

Este propósito busca establecer una estructura que salvaguarde la integridad, confidencialidad y disponibilidad de la información en concordancia con las directrices del MSPI. Se pretende, además, integrar de manera coherente los principios y requisitos de la NTC/IEC ISO 27001, a fin de asegurar un enfoque sistemático y eficiente en la gestión de la seguridad de la información.

Asimismo, busca no solo cumplir con los estándares internacionales, sino también adaptarse a las dinámicas y desafíos específicos del entorno digital. La consideración de los criterios de Continuidad de la Operación, refuerza la resiliencia de los servicios, asegurando que, en situaciones adversas, la entidad pueda mantener la prestación de sus funciones críticas de manera ininterrumpida.

Este enfoque integral no se limita al cumplimiento normativo. La implementación eficaz de estas actividades no solo fortalecerá la seguridad y privacidad de la información en los procesos internos, sino que también contribuirá significativamente a generar confianza.

ALCANCE

El alcance de este documento abarca todos los procesos de la Supersolidaria con el objetivo de asegurar el cumplimiento de lo dispuesto en el Decreto 612 de 2018, en concordancia con la Política de Gobierno Digital y su correspondiente Modelo de Seguridad y Privacidad de la Información, alineados con los estándares de la NTC/IEC ISO 27001. Asimismo, se vincula estrechamente con la estrategia de Seguridad Digital del Estado colombiano.

Este enfoque tiene como propósito garantizar una implementación coherente y eficaz de las medidas de seguridad y privacidad de la información en todas las facetas operativas de la Superintendencia de la Economía Solidaria. La adopción a las normativas y estándares tanto nacionales como internacionales refleja el compromiso de la Supersolidaria con las mejores prácticas y la gestión de la seguridad de la información. La alineación estratégica con la política y la estrategia de seguridad digital del Estado colombiano refuerza la posición de la Entidad, contribuyendo a la consolidación de un entorno digital seguro y robusto.

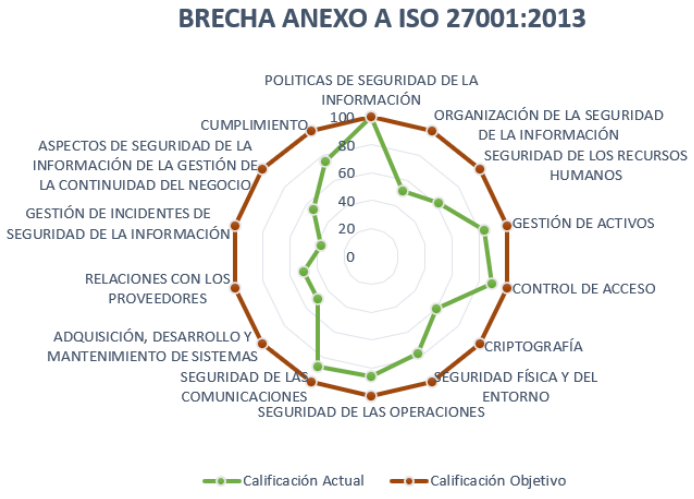
NORMATIVIDAD

- **Constitución Política de Colombia.** Artículos 15, 20, 23 y 74.
- **Ley 1712 de 2014.** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- **Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Ley 1273 de 2009.** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **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.
- **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.
- **Decreto 612 de 2018.** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- **Decreto 1068 de 2015.** Por medio del cual se expide el Decreto Único Reglamentario del Sector Hacienda y Crédito Público.
- **Decreto 886 de 2014.** Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- **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
- **CONPES 3995 de 2020.** Confianza y Seguridad Digital
- **CONPES 3854 de 2017.** Política Nacional de Seguridad digital.
- **CONPES 3701 de 2011**. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **Directiva 26 de 2020.** Diligenciamiento de la información en el índice de transparencia y acceso a la información – ITA – de conformidad con las disposiciones del artículo 23 de la ley 1712 de 2014.

ESTADO ACTUAL DE LA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Según la evaluación interna realizada mediante el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información de la Política Nacional de Gobierno Digital, se ha determinado que el grado de efectividad en la implementación de los controles establecidos por la Norma NTC/ISO 27001:2013 el nivel de avance es el siguiente:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	52	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	62	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	83	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	89	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	60	100	EFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	77	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	86	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	88	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	49	100	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	50	100	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	37	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	54	100	EFECTIVO
A.18	CUMPLIMIENTO	76	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		**69**	**100**	GESTIONADO



POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Superintendencia de la Economía Solidaria, en virtud de la adopción del Modelo de Seguridad y Privacidad de la Información mediante el acta 21 del 2021 del comité de gestión y desempeño, se compromete a salvaguardar, preservar y administrar la privacidad, integridad, disponibilidad y no repudio de la información. Esto se lleva a cabo a través de una gestión integral de riesgos y la aplicación de controles tanto físicos como digitales, con el propósito de prevenir incidentes, garantizar la continuidad de la operación de los servicios y cumplir con los requisitos legales, reglamentarios y regulatorios.

En este sentido, la Superintendencia se esfuerza por mantener un enfoque proactivo en la identificación y mitigación de riesgos, implementando políticas y prácticas que aseguren la robustez de sus sistemas de información. Además, se compromete a fortalecer la resiliencia organizacional mediante la respuesta efectiva a posibles incidentes, con el objetivo de minimizar impactos y garantizar la continuidad operativa de sus servicios esenciales.

La aplicación de controles físicos y digitales se concibe como una estrategia integral, abordando tanto los aspectos tecnológicos como aquellos relacionados con la infraestructura y los recursos humanos. De esta manera, se busca crear un entorno seguro que resguarde la información confidencial y sensible, al tiempo que se fomente una cultura organizacional orientada a la seguridad y la protección de la privacidad.

En línea con los principios de mejora continua, la Superintendencia de la Economía Solidaria se compromete a evaluar regularmente sus políticas y procedimientos de seguridad y privacidad, ajustándolos según las evoluciones tecnológicas y las mejores prácticas del sector. Este enfoque dinámico asegura que la entidad esté siempre a la vanguardia en la protección de la información, adaptándose de manera ágil a un entorno digital en constante cambio.

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

El Plan de implementación de Seguridad y Privacidad de la Información se ejecuta de acuerdo con el siguiente cronograma.

Gestión	Actividad	Tarea	responsable	Fechas	
				Inicio	Fin
Activos de Información	Establecer pautas para la identificación y registro de activos de información.	Actualizar la metodología de levantamiento de activos de información.	Oficial de seguridad de la información.	01-mar	31-mar
	Levantamiento Activos de Información	Socializar la metodología de activos de Información.	Oficial de seguridad de la información.	01-may	31-may
		Validar e identificar nuevos activos de información	Líder de proceso, y equipo de seguridad	01-jun	31-ago
	Publicación de Activos de Información	Aprobar los activos de información	Comité de gestión y desempeño	01-oct	30-oct
		Consolidar el inventario de activos de Información.	Oficial de seguridad de la información.	01-jul	05-jul
		Envío del consolidado de activos de información a la oficina jurídica, para la validación del índice de información clasificada y reservada.	Oficial de seguridad de la información.	08-jul	12-jul

Gestión	Actividad	Tarea	responsable	Fechas	
				Inicio	Fin
Riesgos de seguridad de la información y seguridad digital	Actualización de lineamientos de riesgos	Apoyar cuando se requiera la actualización de la política, metodología y lineamientos de la gestión de riesgos	Funcionario de riesgos de seguridad digital	1-feb	1-mar
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital	Revisión y verificación de los riesgos identificados	Funcionario de riesgos de seguridad digital	1-feb	15-mar
	Aceptación de Riesgos Identificados	Aceptación, aprobación riesgos identificados.	Funcionario de riesgos de seguridad digital	15-mar	29-mar
	Publicación	Publicación mapas de riesgos	Líder de riesgos	1-abr	5-abr
	Seguimiento Fase de Tratamiento	Seguimiento de controles de riesgos identificados	Funcionario de riesgos de seguridad digital, Líder de riesgos	1-abr	31-dic
	Monitoreo y Revisión	Medición, presentación y reporte de indicadores	Funcionario de riesgos de seguridad digital, Líder de riesgos	1-abr	31-dic

Gestión	Actividad	Tarea	responsable	Fechas	
				Inicio	Fin
Incidentes de Seguridad y Privacidad de la Información	Definir, Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	Definición del procedimiento de incidentes de seguridad de la información basado en la norma ISO 27035	Funcionario encargado de la gestión de incidentes de seguridad de la información	01-mar	31-mar
		Socializar cuando se requiera el procedimiento a los funcionarios de la OAPS	Funcionario encargado de la gestión de incidentes de seguridad de la información	01-abr	31-dic
		Socializar el procedimiento a los funcionarios y contratistas de la Supersolidaria	Funcionario encargado de la gestión de incidentes de seguridad de la información	01-abr	31-dic
		Seguimiento a los incidentes de seguridad de la información reportados a la mesa de servicio de acuerdo con lo establecido en el procedimiento definido	Oficial de seguridad de la información	01-abr	31-dic
	CSIRT	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno	Oficial de seguridad de la información.	01-feb	31-dic
	Eventos/vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SGSI	Funcionario encargado de la gestión de incidentes de seguridad de la información	01-feb	31-dic

Gestión	Actividad	Tarea	responsable	Fechas	
				Inicio	Fin
Planeación	Revisión Manual Políticas de Seguridad de la Información.	Actualizar cuando se requiera Políticas y documentación del MSPI.	Oficial de seguridad de la información y equipo de seguridad	01-feb	01-nov
		Actualizar el Plan de Seguridad y Privacidad de la Información.	Oficial de seguridad de la información	25-ene	01-feb

Gestión	Actividad	Tarea	responsable	Fechas	
				Inicio	Fin
Gobierno Digital	Gobierno Digital	Actualizar el documento de autodiagnóstico de la entidad	Oficial de seguridad de la información y equipo de seguridad	01-abr	30-abr
		Alinear la documentación de seguridad de la información de la entidad con el Modelo de Seguridad de la Información (MSPI), conforme a la normativa vigente.	Oficial de seguridad de la información y equipo de seguridad	01-feb	31-dic
		Revisar el avance de implementación del Plan de Seguridad Digital en la Entidad	Oficial de seguridad de la información	01-feb	31-may
	CCOCI	Cumplimiento requerimientos infraestructuras críticas del gobierno	Oficial de seguridad de la información	25-ene	31-dic

Gestión	Actividad	Tarea	responsable	Fechas	
				Inicio	Fin
Auditorías Internas y Externas	Participación en las auditorías internas y externas de la norma ISO 27001:2013	Participar en las auditorías internas y externas de la norma ISO 27001:2013 programadas por la oficina de control interno	Todos los procesos	01-feb	31-dic

Gestión	Actividad	Tarea	responsable	Fechas	
				Inicio	Fin
Revisión de los controles de la norma ISO 27001:2013	Revisión de los controles de la norma ISO 27001:2013	Validación de los controles definidos y reportados en la herramienta de autodiagnóstico	Oficial de seguridad de la información	01-feb	31-dic

Gestión	Actividad	Tarea	responsable	Fechas	
				Inicio	Fin
Vulnerabilidades	Definir lineamientos para ejecutar las pruebas de ethical hacking	Definir los lineamientos y el alcance para la realización de pruebas de vulnerabilidades	Oficial de seguridad de la información, OAPS	01-may	20-may
	Contratar el análisis de ethical hacking	Definir estudios previos para realizar el ethical hacking	Oficial de seguridad de la información, OAPS	20-may	15-jun
	Ejecutar las pruebas de vulnerabilidades	Ejecución de ethical hacking de acuerdo con los estudios previos definidos	Oficial de seguridad de la información, OAPS	1-ago	31-ago
	Ejecutar el plan de remediación de acuerdo con las vulnerabilidades identificadas	Ejecutar el plan de remediación de los sistemas y plataforma de acuerdo con los resultados del análisis de vulnerabilidades.	Oficial de seguridad de la información, OAPS	1-sep	30-nov

Gestión	Actividad	Tarea	responsable	Fechas	
				Inicio	Fin
Gestión de datos personales	Recolectar bases de datos	Redactar y emitir un memorando destinado a la recopilación de datos personales, siguiendo los estándares establecidos por la Superintendencia de Industria y Comercio (SIC).	Oficial de Seguridad, OAPS	01-mar	29-mar
	Revisión de bases de datos	Revisar la información recolectada por las áreas para el registro de las bases de datos	Oficial de Seguridad y Privacidad de la Información y lideres de procesos	29-mar	31-dic
	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos con información suministrada por las delegaturas y el levantamiento de activos de información	OAPS	29-mar	31-dic

Gestión	Actividad	Tarea	responsable	Fechas	
				Inicio	Fin
Plan de Continuidad del Negocio	Documentación del Análisis de Impacto de la Operación	Actualización del Análisis de Impacto del Negocio	Equipo de Continuidad del Negocio	01-abr	30-abr
		Publicación del Análisis de Impacto del Negocio	Equipo de Continuidad del Negocio	01-may	31-may
	Documentación de Valoración de Riesgos de Interrupción	Documento Valoración de Riesgos de interrupción para el plan de continuidad de la operación	Equipo de Continuidad del Negocio	01-may	31-jul
		Valoración de Riesgos de interrupción	Equipo de Continuidad del Negocio	01-may	31-jul
	Documentación de Estrategias de Continuidad	Documento Estrategias de Continuidad de la Operación	Equipo de Continuidad del Negocio	01-may	31-jul
		Publicación Estrategias de Continuidad de la Operación	Equipo de Continuidad del Negocio	1-ago	30-ago
	Documentación del Plan de continuidad de la Operación	Crear Documentación del Plan de continuidad de la Operación	Equipo de Continuidad del Negocio	01-abr	30-ago
		Aprobación del Plan de continuidad de la Operación	Equipo de Continuidad del Negocio	1-sep	30-sep

No	Gestión	No	Actividad	Tarea	Responsable	ENERO				FEBRERO				MARZO				ABRIL				MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE			
						S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
1	Activos de Información	a	Establecer pautas para la identificación y registro de activos de información.	Actualizar la metodología de levantamiento de activos de información.	Oficial de seguridad de la información.																																													
		b	Levantamiento Activos de Información	Socializar la metodología de activos de información.	Oficial de seguridad de la información.																																													
				Validar e identificar nuevos activos de información	Líder de proceso, y equipo de seguridad																																												
		c	Publicación de Activos de Información	Aprobar los activos de información.	Comité de gestión y desempeño																																												
				Consolidar el inventario de activos de información.	Oficial de seguridad de la información.																																												
				Envío del consolidado de activos de información a la oficina jurídica, para la validación del índice de información clasificada y reservada.	Oficial de seguridad de la información.																																												
2	Riesgos de seguridad de la información y seguridad digital	a	Actualización de lineamientos de riesgos	Apoyar cuando se requiera la actualización de la política, metodología y lineamientos de la gestión de riesgos	Funcionario de riesgos de seguridad digital																																													
		b	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital	Revisión y verificación de los riesgos identificados	Funcionario de riesgos de seguridad digital																																													
		c	Aceptación de Riesgos Identificados	Aceptación, aprobación riesgos identificados.	Funcionario de riesgos de seguridad digital																																													
		d	Publicación	Publicación mapas de riesgos	Líder de riesgos																																												
		e	Seguimiento Fase de Tratamiento	Seguimiento de controles de riesgos identificados	Funcionario de riesgos de seguridad digital, Líder de riesgos																																												
		f	Monitoreo y Revisión	Medición, presentación y reporte de indicadores	Funcionario de riesgos de seguridad digital, Líder de riesgos																																												
3	Incidentes de Seguridad y Privacidad de la Información	a	Definir, Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	Definición del procedimiento de incidentes de seguridad de la información basado en la norma ISO 27035	Funcionario encargado de la gestión de incidentes de seguridad de la información																																														
				Socializar cuando se requiera el procedimiento a los funcionarios de la OAPS	Funcionario encargado de la gestión de incidentes de seguridad de la información																																													
				Socializar el procedimiento a los funcionarios y contratistas de la Superintendencia.	Funcionario encargado de la gestión de incidentes de seguridad de la información																																												
				Seguimiento a los incidentes de seguridad de la información reportados a la mesa de servicio de acuerdo con lo establecido en el procedimiento definido	Oficial de seguridad de la información																																													
		b	CSIRT	Socializar los boletines informativos de seguridad, integrar con CSIRT de Gobierno	Oficial de seguridad de la información																																													
		c	Eventos/vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SOSI	Funcionario encargado de la gestión de incidentes de seguridad de la información																																													
4	Planeación	a	Revisión Manual Políticas de Seguridad de la Información.	Actualizar cuando se requiera Políticas y documentación del MSPI	Oficial de seguridad de la información y equipo de seguridad																																														
				Actualizar el Plan de Seguridad y Privacidad de la información	Oficial de seguridad de la información																																													
5	Gobierno Digital	a	Gobierno Digital	Actualizar el documento de autodiagnóstico de la entidad	Oficial de seguridad de la información y equipo de seguridad																																														
				Alinear la documentación de seguridad de la información de la entidad con el Modelo de Seguridad de la Información (MSPI), conforme a la normativa vigente.	Oficial de seguridad de la información y equipo de seguridad																																														
				Revisar el avance de implementación del Plan de Seguridad Digital en la Entidad	Oficial de seguridad de la información																																													
		b	CCOCI	Cumplimiento requerimientos infraestructuras críticas del gobierno	Oficial de seguridad de la información																																													
6	Auditorías Internas y Externas	a	Participación en las auditorías internas y externas de la norma ISO 27001:2013	Participar en las auditorías internas y externas de la norma ISO 27001:2013 programadas por la oficina de control interno	Todos los procesos																																														
7	Revisión de los controles de la norma ISO 27001:2013	a	Revisión de los controles de la norma ISO 27001:2013	Validación de los controles definidos y reportados en la herramienta de autodiagnóstico	Oficial de seguridad de la información																																														
8	Vulnerabilidades	a	Definir lineamientos para ejecutar las pruebas de ethical hacking	Definir los lineamientos y el alcance para la realización de pruebas de vulnerabilidades	Oficial de seguridad de la información, Oficina de Planeación y Sistemas																																														
		b	Contratar el análisis de ethical hacking	Definir estudios previos para realizar el ethical hacking	Oficial de seguridad de la información, OAPS																																													
		c	Ejecutar las pruebas de vulnerabilidades	EEjecución de ethical hacking de acuerdo con los estudios previos definidos	Oficial de seguridad de la información, OPAS																																													
		d	Ejecutar el plan de remediación de acuerdo con las vulnerabilidades identificadas	Ejecutar el plan de remediación de los sistemas y plataforma de acuerdo con los resultados del análisis de vulnerabilidades.	Oficial de seguridad de la información, OAPS																																													
9	Gestión de datos personales	a	Recolectar bases de datos	Elaborar y emitir un memorando Redactar y emitir un memorando destinado a la recopilación de datos personales, siguiendo los estándares establecidos por la Superintendencia de Industria y Comercio (SIC).	Oficial de Seguridad y Privacidad de la Información y OAPS																																														
		b	Revisión de bases de datos	Revisar la información recolectada por las áreas para el registro de las bases de datos	Oficial de Seguridad y Privacidad de la Información y líderes de procesos																																													
		c	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos con información suministrada por las delegaturas y el levantamiento de activos de información	OAPS																																												
10	Plan de Continuidad del Negocio	a	Documentación del Análisis de Impacto de la Operación	Actualización del Análisis de Impacto del Negocio	Equipo de Continuidad del Negocio																																													
				Publicación del Análisis de Impacto del Negocio	Equipo de Continuidad del Negocio																																													
		b	Documentación de Valoración de Riesgos de Interrupción	Documento Valoración de Riesgos de interrupción para el plan de continuidad de la operación	Equipo de Continuidad del Negocio																																													
				Valoración de Riesgos de Interrupción	Equipo de Continuidad del Negocio																																													
		c	Documentación de Estrategias de Continuidad	Documento Estrategias de Continuidad de la Operación	Equipo de Continuidad del Negocio																																													
				Publicación Estrategias de Continuidad de la Operación	Equipo de Continuidad del Negocio																																													
		d	Documentación del Plan de continuidad de la Operación	Crear Documentación del Plan de continuidad de la Operación	Equipo de Continuidad del Negocio																																													
				Aprobación del Plan de continuidad de la Operación	Equipo de Continuidad del Negocio																																													