Supersolidaria
Superintendencia de la Economía Solidaria
"Super-Visión" para la transformación

Plan de Seguridad y Privacidad de la Información

El emprendimiento es de todos
Minhacienda

Contenido

1. INTRODUCCION 2
2. OBJETIVO 2
3. CONCEPCIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 2
4. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN 3
4.1 OBJETIVO GENERAL 3
4.2 OBJETIVOS ESPECIFICOS 4
5. POLITICAS OBJETO DEL SGSI 4
6. ALCANCE 6
7. ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN 6
8. RESPONSABILIDADES DE LA ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN 7
9. OFICIAL DE SEGURIDAD DE LA INFORMACIÓN O QUIEN HAGA SUS VECES 8
10. RESPONSABILIDADES DE PROVEEDORES 8
11. MESAS DE TRABAJO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 8
12. CAPACIDAD PARA EL LOGRO DE LOS RESULTADOS PREVISTOS (ISO 27001) 9
13. ANÁLISIS OBJETIVOS DE CONTROL 9
14. CONTROL DE CAMBIOS 17

1. INTRODUCCION

El aumento del uso de las tecnologías de la información y las comunicaciones, está llevando a los ciudadanos a vivir en un entorno digitalizado, situación que genera incertidumbre y riesgo frente a la seguridad digital, lo que conlleva a un especial interés por parte de las diferentes entidades, con el fin de brindar seguridad y confianza en los usuarios.

Siendo la información el principal activo de toda organización, se debe establecer un plan enfocado en la seguridad de la información, con el fin de proteger la privacidad, seguridad y gestión de su ciclo de vida, cumpliendo los mandatos constitucionales y legales, promoviendo la confianza y cooperación de la ciudanía.

La seguridad de la información debe ser un requisito inherente a las actividades y procesos de la Supersolidaria, y no ser una función adicional o no prioritaria; por lo tanto, se deben establecer mecanismos para difundir, revisar, actualizar y consolidar la política de seguridad de la información institucional, los lineamientos, y demás componentes del Sistema de Gestión de la Seguridad de la Información y alinearlos de forma efectiva con los demás sistemas institucionales.

2. OBJETIVO

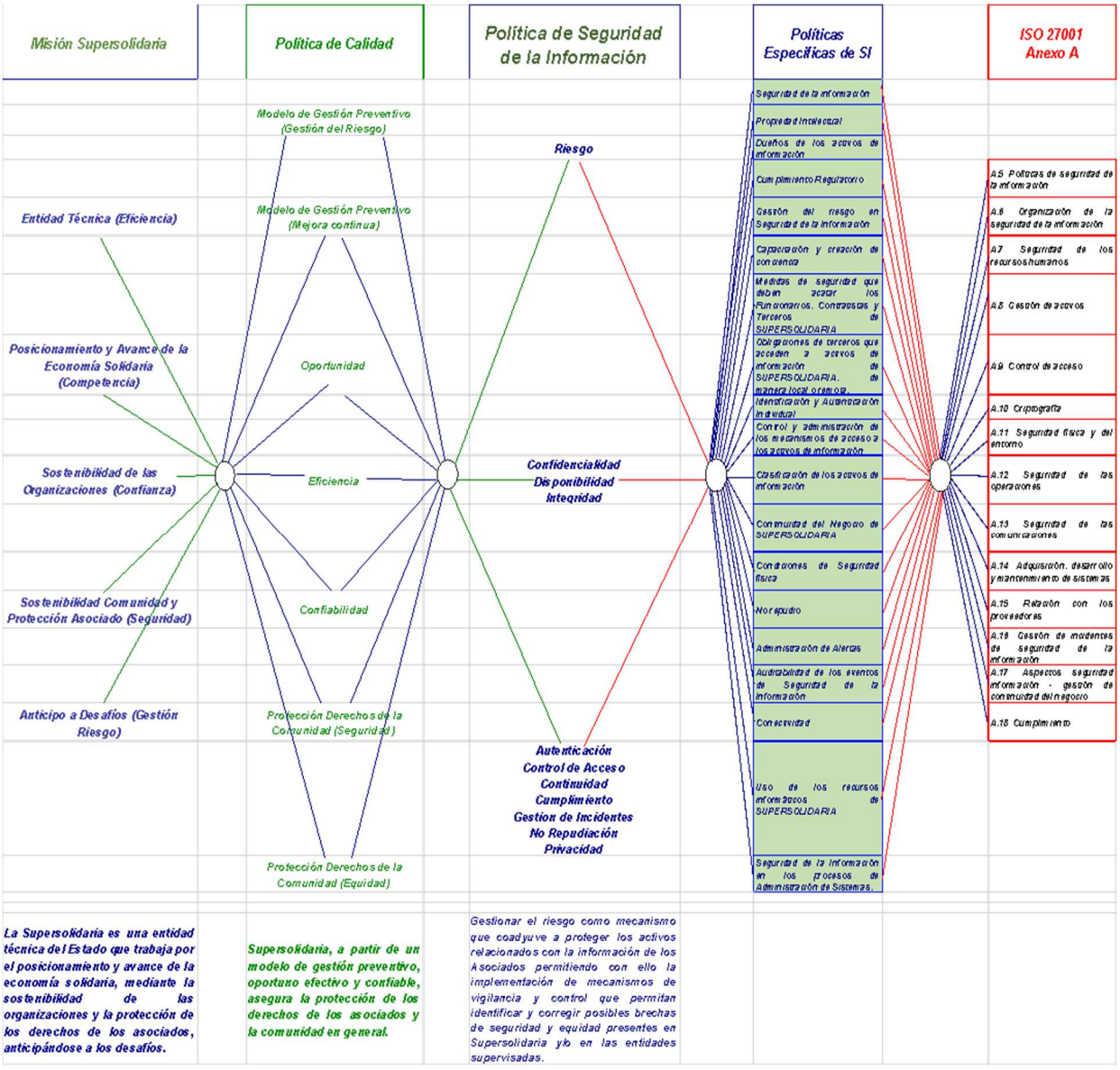
Definir el plan de acción para la implementación del Sistema de Seguridad de la información alineado con el estándar ISO 27001 y los demás sistemas institucionales.

3. CONCEPCIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Para la definición de la política de seguridad de la información, se llevará a cabo una revisión de la Misión de la SUPERSOLIDARIA y su política de calidad presentadas en el Marco Estratégico, así como la práctica en seguridad de la información vigente en el mercado ISO 27000:13, el resultado de ello es una política que pueda aplicarse, implementarse y que se identifique con los intereses de la Superintendencia.

La política deberá permitir:

- Administrar los riesgos en seguridad de la información.
- Definir lineamientos que ayuden a dar tratamiento a los riesgos identificados.
- Establecer los lineamientos para el desarrollo e implantación del Modelo de Seguridad de la Información de la SUPERSOLIDARIA.
- Establecer dueños de los activos de información que soportan los procesos y sistemas de la SUPERSOLIDARIA.
- Condicionar el acceso, uso, manejo y administración de los activos de información.
- Establecer canales que permitan a la Alta Dirección mantenerse informada de los riesgos, uso inadecuado de activos de información, y acciones tomadas para mitigar los riesgos.
- Proteger la reputación, intereses y buen nombre de la SUPERSOLIDARIA.



4. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

4.1 OBJETIVO GENERAL

Cumplir con los requisitos de seguridad, definidos en un sistema de gestión de seguridad de la información, que ayudarán, mediante su implementación, a preservar la confidencialidad, integridad y disponibilidad de la información, así como la relación de los procedimientos asociados a las políticas establecidas que permitan asegurar la protección de esta.

4.2 OBJETIVOS ESPECIFICOS

- Minimizar el riesgo de los procesos misionales de la SUPERSOLIDARIA.
- Cumplir con lo normado en el modelo de seguridad de la información.
- Apoyar la innovación tecnológica y por ende la Misión de la SUPERSOLIDARIA.
- Implementar el sistema de gestión de seguridad de la información (Modelo de Seguridad de la Información).
- Resguardar los activos de información garantizando su aseguramiento físico y digital de la información.
- Establecer las normas, procedimientos y estándares en materia de seguridad de la información.
- Fortalecer la confianza y conciencia en seguridad de la información de los funcionarios, contratistas, terceros, practicantes, entidades vigiladas y Asociados de SUPERSOLIDARIA.
- Garantizar la continuidad de la Superintendencia frente a incidentes.
- Contribuir al incremento de la transparencia, frente a la gestión pública.
- Dar lineamiento para la implementación de la gestión de la seguridad y privacidad de la información.
- Alinear el marco de referencia de arquitectura empresarial con los principios de seguridad y privacidad de la información.

5. POLITICAS OBJETO DEL SGSI

Seguridad de la información:

La Seguridad de la información de la SUPERSOLIDARIA debe estar enmarcada en las medidas de protección y vigilancia requeridas para evitar su divulgación, modificación, hurto o destrucción accidental o maliciosa de información. Las medidas se basan en el valor de la información y el riesgo operacional en que se pueda ver comprometida.

Propiedad intelectual:

Toda licencia, patente, derecho de autor, invención o información que es generado mientras se trabaja en y/o para SUPERSOLIDARIA, se considera de su propiedad intelectual y de uso exclusivo.

Dueños de activos de información:

Es un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.

Cumplimiento regulatorio:

La Política de Seguridad de la Información de la SUPERSOLIDARIA debe alinearse a las exigencias y cumplimiento de las leyes y regulaciones relativas a la Seguridad de la información, todo nuevo requerimiento deberá tenerse en cuenta, ponderarse e implantarse en el Modelo de Seguridad de la Información de la SUPERSOLIDARIA.

SUPERSOLIDARIA toma como mejor práctica de seguridad de la información la norma ISO 27001:13, la cual sirve como base para su modelo de seguridad de la información.

Gestión del riesgo en seguridad de la información

Los riesgos de los activos de información de la SUPERSOLIDARIA serán identificados, evaluados, mitigados y monitoreados acorde con su valor, probabilidad de ocurrencia e impacto.

Los activos de información de la SUPERSOLIDARIA se deberán proteger con base en su valor y riesgo en que puedan verse comprometidos.

Deberá realizarse periódicamente un análisis de riesgo en seguridad de la información sobre: Entidades Vigiladas, Asociados, Terceros, Proveedores y Servicios de SUPERSOLIDARIA, en donde se identifiquen riesgos asociados, dimensionando su impacto y probabilidad. Una vez ha sido aceptado el riesgo por parte del Dueño del Activo

de Información, se actualiza, el valor relativo del activo y el nivel de riesgo a que está expuesto.

Capacitación y toma de conciencia

La SUPERSOLIDARIA deberá establecer un programa de concienciación en seguridad de la información a sus funcionarios, Contratistas y Terceros con los que interactúa.

Funcionarios, Contratistas y Terceros de la SUPERSOLIDARIA deberán estar enterados de los procedimientos de seguridad de la información que aplican en su gestión, así como de las continuas amenazas que ponen en riesgo los activos de información que manejan.

Medidas de seguridad que deberán acatar los funcionarios, Contratistas y Terceros de SUPERSOLIDARIA

La SUPERSOLIDARIA deberá proveer los mecanismos necesarios para asegurar que funcionarios, Contratistas y Terceros cumplen con sus responsabilidades en Seguridad de la Información desde el momento en que se relacionan o vinculan con la SUPERSOLIDARIA hasta su retiro.

6. ALCANCE

Los lineamientos del plan de seguridad y privacidad de la información serán aplicados a los procesos estratégicos, misionales, de apoyo y de evaluación y control de la Supersolidaria, por tal motivo, deberán ser conocidos y cumplidos por todas las partes interesadas, que accedan a los sistemas de información, repositorios e instalaciones físicas.

La Política de Seguridad de la Información da las directrices requeridas para implantar un Modelo de Seguridad de la Información confiable y flexible. Define el marco básico que guía la implantación de cualquier norma, proceso, procedimiento, estándar y/o acción, relacionados.

La Política de Seguridad de la Información debe aplicar para funcionarios, contratistas o terceros, entes externos de control que accedan a la información de la entidad y a todo activo de información creado, procesado o utilizado para el soporte y operación de la SUPERSOLIDARIA, sin importar el medio, formato, presentación o lugar en el que se encuentre.

7. ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

La Supersolidaria designará un Oficial de Seguridad de la Información quien a su vez responderá por la Seguridad Digital de la entidad.

El Oficial de Seguridad de la Información cumple la función de supervisar el cumplimiento de la política, coordinar el Comité de Seguridad de la Información y de asesorar en la materia a los integrantes de la entidad que así lo requieran.

El Oficial de Seguridad de la Información debe mantener y documentar los contactos con autoridades (ColCERT, CSIRT, Centro cibernético Policial, Grupos de atención de desastres, etc.) u otros especializados y asociaciones profesionales para que puedan ser contactados de manera oportuna en el caso de que se presente un incidente de seguridad de la información que requiera de asesoría externa, siempre que esta sea informada por el líder del proceso afectado.

El Oficial de Seguridad de la Información en conjunto con la Oficina Asesora de Comunicaciones deben diseñar e implementar un plan de cambio y cultura organizacional en apropiación del SGSI.

Entre las principales funciones del oficial de seguridad de la información son:

- Mantener actualizadas las políticas de seguridad de la información.
- Definir el procedimiento para la identificación y valoración de activos.
- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
- Asesorar y acompañar a las diferentes líneas de defensa en la gestión de riesgos de seguridad digital, el establecimiento de controles para mitigar los riesgos y el reporte.
- Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.

- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.
- Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad.
- Desarrollar el plan de sensibilización de la entidad incorporando el componente de seguridad de la información.
- Participar en el proceso de elaboración, revisión y evaluación de los procesos contractuales de infraestructura tecnológica.
- Emitir recomendaciones técnicas resultado del proceso de revisión de la plataforma tecnológica y de comunicaciones de la entidad, durante la ejecución del contrato.
- Monitorear de manera permanente las soluciones de seguridad informática existentes en la entidad y aplicar los controles que sean necesarios.
- Identificar, hacer seguimiento y reportar los incidentes de seguridad informática e información presentados en la plataforma institucional.

Correspondiente al proceso de creación de políticas, aprobación y actualización de políticas, se determina:

Creación de políticas: En la Supersolidaria deben ser creadas por el área encargada de la seguridad y privacidad de la información y respaldadas por la Alta Dirección de la entidad con la asesoría de las áreas técnicas responsables de los temas asociados a las mismas.

Aprobación de políticas: En la Supersolidaria las políticas relacionadas con la seguridad y privacidad de la información deben ser aprobadas por la Alta Dirección con base en las recomendaciones del área encargada de la seguridad y privacidad de la información.

Actualización de políticas: En la Supersolidaria las políticas de seguridad y privacidad de la información se deben revisar periódicamente o si ocurren cambios significativos. Cualquier requerimiento de modificación, cambio o actualización de las políticas de seguridad y privacidad de la información, debe ser dirigida a la Alta Dirección con base en las recomendaciones del área encargada.

8. RESPONSABILIDADES DE LA ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

Definir los roles y responsabilidades en seguridad de la información es necesario y requerido para facilitar la implementación del SGSI en la estructura Organizacional de la SUPERSOLIDARIA.

Con el ánimo de lograr el buen funcionamiento del Plan de seguridad y Privacidad de la Información, la Supersolidaria particularizará los roles y responsabilidades de las personas que se van a encargar de establecer y desarrollar cada una de estas actividades asociadas al sistema de seguridad de la información.

Para la asignación de los responsables, la Supersolidaria analizará las funciones de cada rol comparándolas con el personal de la entidad, es necesario que las responsabilidades asignadas en el desarrollo del Sistema de Gestión de Seguridad y Privacidad de la Información para cada perfil sean incorporadas a los manuales de funciones de acuerdo con el cargo que desempeñan.

La administración de esta gestión será responsabilidad del Comité de Seguridad de la Información de la SUPERSOLIDARIA.

9. OFICIAL DE SEGURIDAD DE LA INFORMACIÓN O QUIEN HAGA SUS VECES

Se recomienda a la Supersolidaria, acorde al Decreto 1499 de 2017, designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información en la entidad.

10. RESPONSABILIDADES DE PROVEEDORES

Es responsabilidad de todos los proveedores, que tengan acceso a la información de la Supersolidaria, cumplir con todas las políticas y procedimientos definidos frente a la protección de la información, las cuales le hayan sido suministrados para la labor designada y así mismo usar de manera segura los activos de información que le fueran asignados. Estos proveedores deben estar autorizados por el responsable o líder del proceso, quien será el gestor del control y vigilancia del uso adecuado de los activos de información. Los proveedores deben aceptar por escrito los términos y condiciones de uso de los activos de información, así como el cumplimiento estricto de las políticas de seguridad de la información de la Supersolidaria antes de su acceso a los mismos.

11. MESAS DE TRABAJO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Las Mesas de Trabajo de Seguridad y Privacidad de la Información garantizarán el apoyo y toma de decisiones al proceso de definición, implementación, operación, seguimiento, revisión, mantenimiento y mejora del sistema de gestión de seguridad y privacidad de la información, por lo cual se recomienda conformarlas a través de un equipo de trabajo con funciones determinadas.

12. CAPACIDAD PARA EL LOGRO DE LOS RESULTADOS PREVISTOS (ISO 27001)

SUPERSOLIDARIA toma como mejor práctica de seguridad de la información la norma ISO 27001:13, la cual sirve como base para su modelo de seguridad de la información y debe ser aceptada y referida formalmente como condiciones de gobierno corporativo.

13. ANÁLISIS OBJETIVOS DE CONTROL

A continuación, se presenta el inventario de objetivos de control de establecidos por la norma ISO 27001 y los controles aplicables en cada caso.

ISO 27002	Objetivo de Control	Control
A.5. 1. 1	Políticas para la seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
A.5. 1. 2	Revisión de las políticas para seguridad de la información	Las políticas para seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacias continuas.
A.6. 1. 1	Roles y responsabilidades para la seguridad de información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
A.6. 1. 2	Separación de deberes	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6. 1. 3	Contacto con las autoridades	Se deben mantener los contactos apropiados con las autoridades pertinentes
A.6. 1. 4	Contacto con grupos de interés especial	Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
A.6. 1. 5	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.6. 2. 1	Política para dispositivos móviles	Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6. 2. 2	Teletrabajo	Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.

ISO 27002	Objetivo de Control	Control
A.7. 1. 1	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
A.7. 1. 2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información
A.7. 2. 1	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7. 2. 2	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo
A.7. 2. 3	Proceso disciplinario	Se debe contar con un proceso disciplinario formal el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.7. 3. 1	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.
A.8. 1. 1	Inventario de activos	Se debe identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
A.8. 1. 2	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario.
A.8. 1. 3	Uso aceptable de los activos	Se deber identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8. 1. 4	Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8. 2. 1	Clasificación de la información	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8. 2. 2	Etiquetado de la información	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptada por la organización.
A.8. 2. 3	Manejo de activos	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.

ISO 27002	Objetivo de Control	Control
A.8. 3. 1	Gestión de medios removibles	Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8. 3. 2	Disposición de los medios	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A.8. 3. 3	Transferencia de medios físicos	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A.9. 1. 1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.9. 1. 2	Política sobre el uso de los servicios de red	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9. 2. 1	Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9. 2. 2	Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
A.9. 2. 3	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9. 2. 4	Gestión de información de autenticación secreta de usuarios	La asignación de la información secreta se debe controlar por medio de un proceso de gestión formal.
A.9. 2. 5	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
A.9. 2. 6	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
A.9. 3. 1	Uso de la información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.9. 4. 1	Restricción de acceso Información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso teniendo en cuenta los roles y perfiles de cada sistema de información.
A.9. 4. 2	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
A.9. 4. 3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
A.9. 4. 4	Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
A.9. 4. 5	Control de acceso a códigos fuente de programas	Se debe restringir el acceso a los códigos fuente de los programas.
A.10.1. 1	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

ISO 27002	Objetivo de Control	Control
A.10.1. 2	Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
A.11.1. 1	Perímetro de seguridad física	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.
A.11.1. 2	Controles físicos de entrada	Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
A.11.1. 3	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1. 4	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. El cual debe estar alineado con el plan de continuidad de negocio de la entidad, así como el Plan de Recuperación de Desastres, BCP y DRP.
A.11.1. 5	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.11.1. 6	Áreas de despacho y carga	Se deben controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.11.2. 1	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
A.11.2. 2	Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.11.2. 3	Seguridad del cableado	El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debe estar protegido contra interceptación, interferencia o daño.
A.11.2. 4	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas. Contar con un cronograma de mantenimiento de equipos.
A.11.2. 5	Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
A.11.2. 6	Seguridad de equipos y activos fuera de las instalaciones	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.11.2. 7	Disposición segura o reutilización de equipos	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
A.11.2. 8	Equipos de usuario desatendidos	Los usuarios deben asegurarse de que a los equipos desatendidos se les dé protección apropiada. Los equipos se deben bloquear automáticamente tras inactividad.
A.11.2. 9	Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.

ISO 27002	Objetivo de Control	Control
A.12.1. 1	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.
A.12.1. 2	Gestión de cambios	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A.12.1. 3	Gestión de capacidad	Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
A.12.1. 4	Separación de los ambientes de desarrollo, pruebas y operación	Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A.12.2. 1	Controles contra códigos maliciosos	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A.12.3. 1	Respaldo de información	Se deben hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada. Las cintas deben resguardarse en un sitio alterno a la entidad.
A.12.4. 1	Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4. 2	Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
A.12.4. 3	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad. Se deben generar logs de auditoría.
A.12.4. 4	sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.
A.12.5. 1	Instalación de software en sistemas operativos	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.12.6. 1	Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.12.6. 2	Restricciones sobre la instalación de software	Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios. El software será instalado únicamente a través de un perfil Administrador, gestionado por el área de sistemas.
A.12.7. 1	Información controles de auditoría de sistemas	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13.1. 1	Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.

ISO 27002	Objetivo de Control	Control
A.13.1. 2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
A.13.1. 3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
A.13.2. 1	Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
A.13.2. 2	Acuerdos sobre transferencia de información	Los acuerdos deben tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.
A.13.2. 3	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.
A.13.2. 4	Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14.1. 1	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.14.1. 2	Seguridad de servicios de las aplicaciones en redes publicas	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
A.14.1. 3	Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2. 1	Política de desarrollo seguro	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.
A.14.2. 2	Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2. 3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2. 4	Restricciones en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
A.14.2. 5	Principios de construcción de sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.

ISO 27002	Objetivo de Control	Control
A.14.2. 6	Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2. 7	Desarrollo contratado externamente	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
A.14.2. 8	Pruebas de seguridad de sistemas	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2. 9	Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.
A.14.3. 1	Protección de datos de prueba	Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.
A.15.1. 1	Política de seguridad de la información para las relaciones con proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.
A.15.1. 2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
A.15.1. 3	Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
A.15.2. 1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A.15.2. 2	Gestión de cambios en los servicios de proveedores	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.
A.16.1. 1	Responsabilidad y procedimientos	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1. 2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A.16.1. 3	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
A.16.1. 4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.
A.16.1. 5	Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.

ISO 27002	Objetivo de Control	Control
A.16.1. 6	Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.
A.16.1. 7	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17.1. 1	Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1. 2	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
A.17.1. 3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2. 1	Disponibilidad de instalaciones de procesamiento de información.	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
A.18.1. 1	Identificación de la legislación aplicable y de los requisitos contractuales	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
A.18.1. 2	Derechos de propiedad intelectual	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A.18.1. 3	Protección de registros	Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1. 4	Privacidad y protección de datos personales	Cuando sea aplicable, se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.
A.18.1. 5	Reglamentación de controles criptográficos	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A.18.2. 1	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.

ISO 27002	Objetivo de Control	Control
A.18.2. 2	Cumplimiento con las políticas y normas de seguridad	La alta dirección debe revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A.18.2. 3	Revisión del cumplimiento técnico	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

14. CONTROL DE CAMBIOS

Fecha	Descripción del cambio
Diciembre 26 de 2021	Actualización del Plan por cambio de vigencia 2021