

 COOPERATIVA DE AHORRO Y CRÉDITO COOPEAYPE <i>Empresa de Proyección Alpuna</i>	PROCESO	GESTIÓN DE SISTEMAS			
	MANUAL	MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACION PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS			
	Código	SI-MA-1	Versión	1	Emisión marzo/2022 pagina 1 de 26

COOPERATIVA DE AHORRO Y CRÉDITO COOPEAYPE

ACUERDO No. 38 DE 02 ABRIL DE 2022

Por el cual se aprueba el **MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACION PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS**

El Consejo de Administración de COOPEAYPE, en uso de sus facultades legales y estatutarias y,

CONSIDERANDO

- Que, es deber del Consejo de Administración, proferir los actos Administrativos necesarios para el normal desarrollo del objeto social de la Entidad.
- Que, de acuerdo con el TÍTULO IV SISTEMA DE ADMINISTRACIÓN DE RIESGOS CAPÍTULO IV SISTEMA DE ADMINISTRACIÓN DEL RIESGO OPERATIVO – SARO ANEXO 2 INSTRUCCIONES SOBRE SEGURIDAD Y CALIDAD DE LA INFORMACION PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS de la Circular Básica Contable y Financiera se debe adoptar una política de buenas prácticas en materia de seguridad de la información, que les permita identificar los riesgos operativos tecnológicos, así como la posible materialización de incidentes de seguridad que pongan en riesgo la confidencialidad, integridad y disponibilidad de los activos de información, y se adopten, de manera preventiva, los mecanismos que minimicen su impacto, como un elemento que fortalezca la confianza de las organizaciones que conforman el sector solidario actual
- Que, en vista de lo anterior

ACUERDA:

Artículo 1. Aprobar la Versión 01 del **Manual De La Seguridad Y Calidad De La Información Para La Prestación De Los Servicios Financieros** para COOPEAYPE, código **SIMA1 MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACION PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS V1** anexo 1, así mismo lo no previsto en ellos se regirá por las leyes vigentes sobre la materia.

Artículo 2. ÁMBITO DE APLICACIÓN: El presente manual será aplicable a todos los miembros del Consejo de Administración, Junta de vigilancia, comités especializados, funcionarios y, en general, a todos los asociados de la Cooperativa de Ahorro y Crédito COOPEAYPE.

Artículo 3. CONFIDENCIALIDAD Y MANEJO DE INFORMACIÓN: Las actuaciones contempladas en este manual, son de estricto carácter confidencial y, en consecuencia, no deberá divulgarlas individualmente, por lo tanto, los asuntos o decisiones tratados o

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 COOPEAIPe <i>Empresa de Proyección Alpuna</i>	PROCESO	GESTIÓN DE SISTEMAS				
	MANUAL	MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022
		página	2 de 26			

adoptados, así como todos los aspectos internos de **COOPEAIPe** relacionados, solamente podrán ser dados a conocer a través de los canales formales de comunicación de **COOPEAIPe** y únicamente a las personas, órganos o entidades a quienes corresponda conocerlos.

Artículo 4. APPLICACIÓN DE NORMAS SUPERIORES: Los casos no previstos en este manual y que no hayan sido desarrollados mediante reglamentaciones internas, se resolverán conforme a la Ley o Decretos especiales y concordantes sobre la materia, las normas emanadas de la Supersolidaria o el Organismo competente.

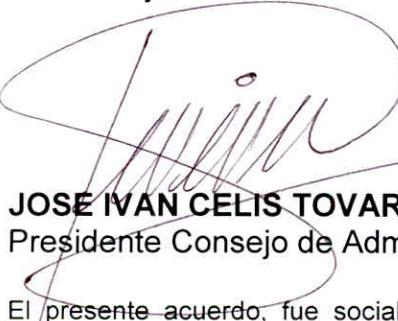
Artículo 5. MODIFICACIONES: Cualquier modificación parcial o total se realizará por convocatoria del Consejo de Administración y justificada por acto Administrativo (Acuerdo) y la decisión debe ser unánime y los ajustes realizados sólo tendrán validez a partir de la fecha de aprobación de este organismo. En todo caso se tomarán en cuenta las normas vigentes, en especial las que guardan relación con la Circular Básica Contable y Financiera expedida por la Supersolidaria, y/o las normas o circulares que lo complementen, modifiquen o sustituyan.

Artículo 6. NORMAS APLICABLES: además de las normas del presente manual, se ceñirá a las que sean pertinente de la legislación cooperativa y solidaria, el Estatuto u otros reglamento interno o mandatos especiales de la Asamblea General o a normas de cumplimiento obligatorio emanadas de autoridades competentes.

Artículo 7. MATERIAS NO REGULADAS: las materias y situaciones no reguladas en el presente Código, así como las dudas de interpretación, serán resueltas por el Consejo de Administración de **COOPEAIPe** con el voto favorable de la mayoría absoluta (las dos terceras 2/3 partes) de los asistentes

Artículo 8. Vigencia el presente manual rige a partir de la fecha de su aprobación, por parte del Consejo de Administración y deroga todas las normas anteriores sobre la materia.

Artículo 9. El presente manual fue socializado y aprobado en reunión extraordinaria 07 de Consejo de Administración en sesión realizada el 02 de abril de 2022.



JOSE IVAN CELIS TOVAR
Presidente Consejo de Administración



AGUSTIN CHARRY CHARRY
secretario Consejo de Administración

El presente acuerdo, fue socializado y aprobado por el Consejo de Administración, en uso de sus facultades legales, estatutarias y reglamentarias, en reunión del día 02 del mes de abril del año 2022, y según consta en el acta extraordinaria número 07 de 2022.

	PROCESO	GESTIÓN DE SISTEMAS				
	MANUAL	MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022
		página		3 de 26		

ANEXO 1

MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS

1. OBJETIVO.

Establecer y mantener políticas, controles y programas que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información, asegurando que los recursos de los Sistemas de Información (material informático o programas), sean utilizados de la forma en que se decidió y que la información que se considera importante o sensible no sea fácil de acceder por cualquier persona no autorizada.

2. ALCANCE.

Aplica para todos los directivos, funcionarios fijos y temporales, contratistas y otras personas que utilicen la plataforma tecnológica y cualquier tipo de información física y de servicios tecnológicos de COOPEAIPE.

3. NORMATIVIDAD.

3.1. EXTERNA.

- 3.1.1. Circular Básica Contable y Financiera TÍTULO IV SISTEMA DE ADMINISTRACIÓN DE RIESGOS, CAPÍTULO IV SISTEMA DE ADMINISTRACIÓN DEL RIESGO OPERATIVO – SARO, ANEXO 2 INSTRUCCIONES SOBRE SEGURIDAD Y CALIDAD DE LA INFORMACION PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS expedida por la SUPERSOLIDARIA.
- 3.1.2. **Ley 1952 de 2019:** por medio de la cual se expide los PRINCIPIOS Y NORMAS RECTORAS DE LA LEY DISCIPLINARIA y se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario.
- 3.1.3. **Ley 603 de 2000:** Esta Ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.
- 3.1.4. **Ley Estatutaria 1266 del 31 de diciembre 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.
- 3.1.5. **Ley 1273 del 5 de enero 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

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

	PROCESO	GESTIÓN DE SISTEMAS			
	MANUAL	MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS			
	Código	SI-MA-1	Versión 1	Emisión marzo/2022	pagina 4 de 26

información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Ver esta Ley.

- 3.1.6. **Ley Estatutaria 1581 De 2012:** Entró en vigor la Ley 1581 del 17 de octubre 2012 de Protección de Datos Personales, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.
- 3.1.7. **Decreto 1377 De 2013:** Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012. Añade dos nuevos capítulos al Código Penal Colombiano:
 - Capítulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos;
 - Capítulo Segundo: De los atentados informáticos y otras infracciones. Como se puede ver en el primer capítulo, esta Ley está muy ligada a la ISO-27000, lo cual coloca al País a la vanguardia en legislación de seguridad de la información, abriendo así la posibilidad de nuevas entradas con este tema.
- 3.1.8. **Ley 1273 DE 2009:** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado "de la protección de la información y los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- 3.1.9. **Decreto No. 2573 de 2014,** establece como lineamiento la Seguridad y privacidad de la Información y comprende acciones transversales además de componentes enunciados, a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada.
- 3.1.10. Norma Técnica Colombiana NTC-ISO-IEC 27001:2013. Norma técnica de sistemas de gestión de seguridad de la información.

4. DEFINICIONES.

- 4.1. **Acción resolutiva:** Acción tomada para evitar la repetición de un incumplimiento mediante la identificación y tratamiento de las causas que la provocaron.
- 4.2. **Activo de información:** Conocimiento o datos que tienen valor para la organización o el individuo.
- 4.3. **Amenaza:** Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización
- 4.4. **Antivirus:** son programas cuya función es detectar y eliminar virus informáticos y programas maliciosos

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 COOPEAIPE <small>Empresa de Proyección Alpuna</small>	PROCESO		GESTIÓN DE SISTEMAS					
	MANUAL		MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACION PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS					
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022	pagina	5 de 26

- 4.5. **Base de datos:** Es un conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente para su posterior uso
- 4.6. **Centro de cómputo:** En esta ubicación se encuentran todos los recursos necesarios para el procesamiento de la información de la Cooperativa como servidores, routers, switches, etc
- 4.7. **Colaboradores:** (funcionarios, contratistas y/o terceros) de todas las áreas y procesos de **COOPEAIPE** y, adicionalmente, por los ciudadanos, persona naturales o jurídicas, nacionales o extranjera que sin tener relación laboral o contractual con **COOPEAIPE** tengan acceso a sus instalaciones y/o servicios tecnológicos.
- 4.8. **Confidencialidad:** Considera que la información no se pone a disposición ni se revela a personal o a entidades no autorizadas.
- 4.9. **Control:** Medida o acción que modifica un riesgo para prevenir su materialización
- 4.10. **Copia de seguridad o Back Ups:** Su objetivo es mantener la capacidad de recuperación de información ante posibles pérdidas.
- 4.11. **Disponibilidad:** Posibilidad de que la información debe estar accesible en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.
- 4.12. **DNS:** es un sistema de nomenclatura jerárquico que se ocupa de la administración del espacio de nombres de dominio (Domain Name Space) consiste en resolver las peticiones de asignación de nombres
- 4.13. **DRP o Plan de Recuperación de Desastres:** Es un sistema con el cual las organizaciones se preparan contra posibles desastres de diversa índole que puedan dañar su infraestructura tecnológica
- 4.14. **Firewall:** Sistema de seguridad que impide que los usuarios no autorizados accedan a la red y por lo tanto a la información alojada en los servidores y equipos de la red.
- 4.15. **Gobierno de seguridad de la información:** Sistema por el cual las actividades de seguridad de la información de una organización son dirigidas y controladas
- 4.16. **Hardware:** Hace referencia a todas las partes tangibles de un sistema informático como disco, teclado, monitor, impresora, entre otros.
- 4.17. **Incidente de Seguridad:** se define como un evento que atenta contra la confidencialidad, integridad y/o disponibilidad de la información y los recursos tecnológicos de la organización.
- 4.18. **Integridad:** La información debe ser precisa, coherente y completa desde su creación hasta su destrucción, debe ser inalterada ante accidentes o intentos maliciosos, siempre se debe prevenir modificaciones no autorizadas de la información
- 4.19. **Internet:** Es un conjunto descentralizado de redes de comunicación interconectadas entre sí.
- 4.20. **Intranet:** Es una interconexión de redes informáticas privadas para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales.

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 COOPEAYPE <small>Empresa de Proyección Aljuna</small>	PROCESO		GESTIÓN DE SISTEMAS				
	MANUAL		MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022	pagina

- 4.21. IP o Internet Protocol (Protocolo de Internet):** es el sistema estándar mediante el cual funciona la internet, por medio de un proceso de envío y recepción de información.
- 4.22. Licencia:** Es un contrato donde una persona recibe el derecho del uso de un bien a cambio de un monto establecido
- 4.23. Logs:** Es un registro de una actividad de un sistema utilizados para verificar, monitorear y detectar errores y validar procesos.
- 4.24. Nivel de riesgo:** Evaluación del riesgo identificando su posible materialización frente al impacto y probabilidad de ocurrencia.
- 4.25. Parches de seguridad:** Son todas las actualizaciones pertinentes a las que se encuentran sometidas todas las aplicaciones y sistemas operativos de una computadora
- 4.26. Password:** Es la clave secreta o personal con la que se accede a la información contenida en un PC o en una red informática.
- 4.27. PCI-DSS:** Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (Payment Card Industry Data Security Standard – PCI DSS)
- 4.28. PIN PAD o dispositivo de entrada de PIN:** es un dispositivo electrónico utilizado en una transacción de débito, crédito o tarjeta inteligente para aceptar y cifrar el número de identificación personal del titular de la tarjeta.
- 4.29. Políticas de seguridad:** Conjunto de directrices, lineamientos y reglas que permiten velar porque se resguarden los activos de información, aprobados por el consejo de administración.
- 4.30. POS:** es una agrupación de diferentes software y hardware que, al combinarse, permiten a las empresas procesar sus transacciones de cara al asociado.
- 4.31. Probabilidad:** Posibilidad que el riesgo se pueda materializar frente a un incidente de seguridad de la información.
- 4.32. Riesgo residual:** Es el riesgo que queda después de aplicar los controles al riesgo identificado.
- 4.33. Seguridad de la información:** Es el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacene, reproduzca o procese en los sistemas informáticos de la organización.
- 4.34. Servicie pack:** o paquete de servicios consiste en un grupo de actualizaciones de constituyen corrigen y mejoran una a aplicación o sistema operativo.
- 4.35. Servicios de computación en la nube:** Modelo para permitir un acceso de red conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo de administración o proveedor de servicios.

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

	PROCESO		GESTIÓN DE SISTEMAS				
	MANUAL		MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022	pagina

- 4.36. **Servidor:** Es un nodo que forma parte de una red y su objetivo es proveer servicios a otros equipos de cómputo llamados clientes. Algunos servicios pueden ser: impresión, correo, mensajería instantánea, entre otros)
- 4.37. **Servidor hosting:** Plataforma en la cual se encuentra alojada la página web de la cooperativa y a la cual podemos acceder vía internet.
- 4.38. **Sistema de Información:** Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- 4.39. **Software:** es el equipamiento lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos (Hardware).
- 4.40. **UPS (Uninterruptible Power Supply) o sistema de alimentación ininterrumpida:** es una fuente de suministro eléctrico que permite brindar energía eléctrica por un tiempo limitado a dispositivos eléctricos/electrónicos en el caso de interrupción eléctrica
- 4.41. **VPN (sigla en inglés para red privada virtual):** es una tecnología que utiliza Internet para conectarse a una ubicación específica y de esta manera poder acceder a ciertos servicios
- 4.42. **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotado por una o más amenazas

5. ELEMENTOS CLAVES DE LA INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACIÓN.

5.1. Gobierno de seguridad de la información

COOPEAIPE definirá y pondrá en marcha el sistema de seguridad de la información como un componente integral de sus prácticas de buen gobierno.

El sistema de seguridad de la información proporciona la dirección estratégica a las actividades de seguridad y garantiza que se alcancen los objetivos y que se realice la debida gestión de los riesgos relacionados con seguridad de la información; igualmente establece que los recursos de información de la Cooperativa se utilicen con responsabilidad. Esta es una responsabilidad del consejo de administración y la alta dirección de la Cooperativa.

5.2. Estrategia de Seguridad

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 COOPEAIPE <small>Empresa de Proyección Alpina</small>	PROCESO		GESTIÓN DE SISTEMAS				
	MANUAL		MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022	pagina 8 de 26

El objetivo de la estrategia de seguridad de la información es alcanzar el estado deseado definido por los atributos de seguridad de la información en la Cooperativa. El plan o planes de acción deben ser formulados sobre la base de los recursos y limitaciones disponibles, incluida la consideración de los requisitos legales y reglamentarios pertinentes.

COOPEAIPE debe definir y documentar una política de seguridad de la información, alineada con la estrategia del negocio, que identifique, como mínimo:

- qué se va a hacer;
- qué recursos se requerirán;
- quién será el responsable;
- cuando finalizará;
- cómo se evaluarán los resultados logrados

6. ROLES Y RESPONSABILIDADES

Sin perjuicio de las funciones asignadas en otras disposiciones, frente al sistema de seguridad de la información les corresponde:

6.1. Consejo de Administración

- Definir y promover la dirección estratégica para la seguridad de la información.
- Proporcionar los recursos para la adecuada implementación de la seguridad de la información.
- Proporcionar, velar y apoyar la implementación y asignación del Sistema de Seguridad de Información.
- Autorizar, facilitar e integrar la puesta en operación del sistema de seguridad de la información, mediante la definición de mecanismos y la supervisión e integración por parte de cada líder de proceso.
- Velar por el cumplimiento de las obligaciones regulatorias en materia de seguridad de la información.
- Velar por la disponibilidad de los recursos y su uso apropiado.
- Designar los responsables de la implementación del sistema de seguridad de la información.
- Pronunciarse y hacer seguimiento a los informes trimestrales que presente el representante legal, dejando constancia en las actas de las reuniones respectivas.
- Aprobar las evaluaciones de riesgo de seguridad de la información resultantes.

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

	PROCESO	GESTIÓN DE SISTEMAS				
	MANUAL	MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022

- Revisar que la estrategia de seguridad de la información se encuentre alineada con los objetivos de negocio.
- Revisar y aprobar las actualizaciones al Sistema de Gestión de Seguridad de la Información (SGSI), para garantizar su continua conveniencia, idoneidad y efectividad.
- Establecer las prioridades de los proyectos e iniciativas relacionadas con la seguridad de la información.

6.2. Representante Legal

- Velar por el desarrollo de los objetivos estratégicos para la seguridad de la información, definidos por el consejo de administración.
- Velar por la implementación de la política de seguridad de la información.
- Facilitar la integración entre los diferentes dueños de procesos de negocio para lograr la implementación del modelo de seguridad de la información.
- Velar por la disponibilidad de los recursos y su uso apropiado.
- Velar por la correcta aplicación de los controles de seguridad para reducir el riesgo de seguridad de la información
- Velar por la designación de los responsables de la implementación de la política de seguridad de la información.
- Presentar un informe periódico, como mínimo trimestral, al Consejo de Administración sobre la evolución y aspectos relevantes de la seguridad de la información incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar, seguimiento y resultados de mediciones y cumplimiento de objetivos de seguridad de la información.

6.3. Auditoría interna o quien ejerza control interno

- Tener conocimiento apropiado en materia de seguridad de la información y de esta normativa en particular.
- Evaluar periódicamente la efectividad y cumplimiento de todas y cada una de las etapas y los elementos clave del sistema de seguridad de la información, con el fin de determinar las deficiencias y sus posibles soluciones.
- Informar los resultados de la evaluación de la seguridad de la información al consejo de administración.

6.4. Estándar base para adaptar el Sistema de Seguridad de la Información

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

 COOPEAIPE <i>Empresa de Proyección Alpuna</i>	PROCESO		GESTIÓN DE SISTEMAS					
	MANUAL		MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS					
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022	pagina	10 de 26

COOPEAIPE adoptara un Modelo de Seguridad y Privacidad de la Información, que permita el aseguramiento de los activos de información y que contemple elementos para establecer, implementar, mantener y proveer mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI). Para tal efecto, se tomará como referencia el estándar de seguridad de la información ISO27001 de 2013.

7. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión de riesgos es un proceso encaminado a minimizar las vulnerabilidades y posibles pérdidas de información que pueden llegar a materializarse y afectar económica y reputacionalmente a La Cooperativa. Para tal efecto, se deben establecer niveles aceptables de aseguramiento y previsibilidad sobre los resultados deseados de cualquier actividad importante de COOPEAIPE y llevar a cabo un proceso sistemático que permita:

- Tener comprensión de las amenazas, las vulnerabilidades, y el perfil de riesgo de la Cooperativa.
- Tener entendimiento de la exposición al riesgo y las posibles consecuencias para el negocio.
- Crear conciencia de las prioridades de la gestión de riesgos con base en las posibles consecuencias de materialización.
- Definir e implementar estrategias organizacionales adecuadas para la mitigación de riesgos para obtener consecuencias aceptables.
- Fijar la atención organizacional con base en un entendimiento de las posibles consecuencias del riesgo residual.
- Conservar información documentada del proceso de gestión de riesgos de seguridad de la información.

8. SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

COOPEAIPE cuenta con políticas que identifican el contexto y los objetivos propios, atendiendo como mínimo lo siguiente:

8.1. Descripción

El proceso de descripción de las políticas de seguridad de la información implica que bajo un lenguaje conciso y de fácil comprensión, se identifiquen e incorporen los temas propios de seguridad, normativa aplicable, tipo de información sensible,

	PROCESO		GESTIÓN DE SISTEMAS					
	MANUAL		MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS					
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022	pagina	11 de 26

identificación de la clasificación de la información, responsables y niveles de autorización.

8.2. Revisión

El proceso de revisión debe contemplar la aplicación de actividades de retroalimentación como soporte de conocimiento que permitan la socialización y la verificación del cumplimiento de las políticas de seguridad, alineadas con los objetivos de la Cooperativa

8.3. Aprobación

Este proceso está a cargo del consejo de administración o, quien haga sus veces, en la Cooperativa, quien emitirá la aprobación de las políticas del Sistema de Seguridad de Información y establecerá las instrucciones para su puesta en marcha y cumplimiento.

8.4. Publicación

Cumplidos los procesos de descripción, revisión y aprobación, COOPEAIPE dará a conocer las políticas de seguridad de la información, las cuales deberán ser publicadas a través de los medios de comunicación que habitualmente utiliza, siendo necesario que se apliquen estrategias que faciliten su difusión y su contenido por todos y cada uno de los integrantes de la Cooperativa.

8.5. Evaluación

COOPEAIPE deberá aplicar evaluaciones de conocimiento al personal, garantizando que las políticas son leídas y se aplican de acuerdo con lo establecido.

8.6. Actualización

El desarrollo de la Seguridad de Información debe considerarse como un proceso de mejora continua, por lo cual, al aplicar los controles de seguridad bajo parámetros previamente establecidos para su medición, debe generar como resultado los aspectos a corregir, los cambios que se deben realizar o, la identificación de nuevos riesgos. De igual forma, el resultado de las evaluaciones y verificaciones que evidencien el recurrente incumplimiento a las políticas, la recepción de sugerencias por las partes interesadas y la oportunidad de cambios tecnológicos al interior de la

	PROCESO		GESTIÓN DE SISTEMAS				
	MANUAL		MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022	pagina

Cooperativa, le permitirán a esta tomar decisión en relación con la necesidad de llevar a cabo procesos de actualización de dichas políticas.

9. RECURSOS

COOPEAIPe determinará y proporcionará los recursos necesarios para el establecimiento e implementación del Sistema de Seguridad de la Información, que considere los siguientes aspectos:

9.1. Presupuesto

El presupuesto deberá contemplar la criticidad de los activos de información involucrados, y los recursos que aseguren la función de seguridad de la información, las herramientas tecnológicas que apoyen a la protección de los activos de información y el proceso de mejora continua.

9.2. Competencia

COOPEAIPe debe procurar que los responsables de la seguridad de la información cuenten con la competencia necesaria para gestionar los riesgos asociados, evaluar la eficacia de las acciones tomadas y garantizar la información documentada.

9.3. Comunicación

La comunicación es especialmente importante entre todas las partes interesadas dentro de las cadenas de suministro, por lo que el Sistema de Seguridad de Información debe proporcionar un medio para comunicar los requisitos exigidos, entre los responsables de la entrega de productos y servicios esenciales de la Cooperativa.

10. INFORMACIÓN DOCUMENTADA

El modelo de seguridad de la información de la Cooperativa vigilada debe incluir la información documentada requerida por esta norma, considerando los siguientes componentes:

10.1. Principios de seguridad de la información

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

	PROCESO		GESTIÓN DE SISTEMAS					
	MANUAL		MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS					
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022	página	13 de 26

El consejo de administración tiene la responsabilidad de aprobar una política general de seguridad de la información, la cual debe estar disponible para ser entregada a los organismos de vigilancia y control, teniendo en cuenta que:

- Esté adecuada al propósito de la Cooperativa vigilada.
- Incluya objetivos de seguridad de la información o proporcione el marco de referencia para el establecimiento de los objetivos de la seguridad de la información.
- Incluya el compromiso de cumplir los requisitos aplicables relacionados con la seguridad de la información.
- Incluya el compromiso de mejora continua del sistema de seguridad de la información.
- Esté disponible como información documentada.
- Se comunique dentro de la Cooperativa.
- Esté disponible para las partes interesadas, según sea apropiado.

10.2. Otra información documentada

El modelo de seguridad de la información de la Cooperativa debe estar acompañado por otro tipo de información documentada como:

- Procedimientos de seguridad.
- Instructivos o guías técnicas.

10.3. Creación y actualización de la información documentada

Cuando se crea y actualiza información documentada del sistema de seguridad, COOPEAIPE debe asegurarse de que sea apropiado e incluya:

- La identificación y descripción (por ejemplo: título, fecha, autor o número de referencia)
- El formato (versión del software, gráficos) y sus medios de soporte (por ejemplo: papel, electrónico)
- La revisión y aprobación con respecto a la idoneidad y adecuación.

10.4. Control de la información documentada

La información documentada requerida por el sistema de seguridad de la información, se debe controlar para asegurarse de que esté disponible, adecuada

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

	PROCESO		GESTIÓN DE SISTEMAS				
	MANUAL		MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022	pagina

para su uso y esté protegida adecuadamente, entre otros, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad. El control debe efectuarse sobre la distribución, acceso, recuperación y uso de almacenamiento y preservación, incluida la preservación de la legibilidad, control de cambios, retención y disposición.

11. RESPONSABILIDADES Y RECURSOS

11.1. Roles y Responsabilidades

COOPEAIPE debe tener una clara definición de los roles y responsabilidades asignadas a funcionarios acorde a las funciones del cargo. Cada rol debe tener responsabilidad específica con respecto al riesgo y la seguridad de la información.

11.2. Recursos humanos

COOPEAIPE debe tener definidos claramente los términos y condiciones de los cargos asociados a la seguridad de la información entre profesionales de la seguridad, los administradores de redes / sistemas de TI, la alta gerencia, los auditores (interno y externos) y los trabajadores en general, respecto a las funciones y responsabilidades en la seguridad de la información. Adicionalmente, es conveniente contar con un programa de concientización/educación sobre la seguridad de la información extendido a directivos y trabajadores, para lo cual será necesario:

- Proveer toda la información a los funcionarios sobre la postura, estrategias y políticas de seguridad de la información de la Cooperativa.
- Implementar un proceso disciplinario para incidentes de seguridad de la información, violaciones a la privacidad, piratería informática, fraude y espionaje industrial, por parte de los trabajadores, el cual deberá ser informado a estos desde el proceso de inducción.
- Se deberán tener en cuenta las promociones, degradaciones, cambios de roles, nuevas responsabilidades, nuevas prácticas de trabajo, renuncias y despidos.

12. REQUERIMIENTOS DE MEDIOS TECNOLÓGICOS Y SEGURIDAD DE LA INFORMACIÓN

En desarrollo de los criterios de seguridad para los medios tecnológicos y considerando los canales de distribución utilizados, COOPEAIPE deberá cumplir, como mínimo, con los siguientes requerimientos:

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

	PROCESO		GESTIÓN DE SISTEMAS				
	MANUAL		MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022	pagina 15 de 26

- Disponer de hardware, software y equipos de telecomunicaciones que mitiguen las amenazas del sector, y crear procedimientos y controles necesarios que permitan la prestación de los servicios y el manejo de la información, en condiciones de seguridad y calidad.
- Gestionar la seguridad de la información bajo un Modelo de Seguridad y Privacidad de la Información.
- Gestionar con sus tarjetahabientes estándares de seguridad tales como PCI-DSS.
- Gestionar mecanismos para el envío de información a sus asociados, tales como: certificaciones, extractos, notificaciones, entre otros, así como los medios (tarjetas débito y crédito, etc.) bajo medidas de seguridad. Cuando la información que la Cooperativa remite a sus asociados sea de carácter confidencial y se envíe como parte o adjunta a un correo electrónico, ésta deberá estar cifrada.
- Garantizar, de manera segura, el registro de las direcciones IP y los números de los teléfonos fijos y móviles desde los cuales operará. La Cooperativa podrá determinar los procedimientos que permitan identificar y, de ser necesario, bloquear las transacciones provenientes de direcciones IP o números fijos o móviles considerados como inseguros.
- Todas las conexiones a aplicaciones de terceros deben estar en mecanismos seguros de conexión como son VPN, canales exclusivos, con el registro de IP por parte de entidades para evitar acceder desde lugares remotos sin la debida seguridad y/o autorización pertinente.

12.1. Controles criptográficos

- Los sitios web creados para el procesamiento de la información, deben ser sitios seguros y utilizar certificados digitales emitidos por un ente certificador legalmente constituido en el país.
- Las comunicaciones con terceras partes para la prestación de servicios deben utilizar mecanismos de encriptación fuertes.
- Se deben utilizar herramientas que cuenten con algoritmos de encriptación en el almacenamiento de la información sensible o crítica en archivos, así como las claves de usuarios a los sistemas de información.

13. PROTECCIÓN CONTRA CÓDIGOS MÓVILES O MALICIOSOS

- Se debe mantener instalado, en los equipos de la Cooperativa, software antivirus los cuales serán actualizados constantemente por parte del área encargada.

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

	PROCESO		GESTIÓN DE SISTEMAS					
	MANUAL		MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS					
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022	pagina	16 de 26

- Evitar o restringir el intercambio de CD's, memorias tipo USB y otros medios removibles de origen desconocido o, si fuere necesario, someterlos a la revisión del antivirus instalado en el disco antes de su utilización.
- Restringir el uso de los equipos por parte de personas ajena s a las actividades propias de la Cooperativa.
- En el caso de los archivos comprimidos bajo el formato ZIP o cualquier otro tipo de archivo que fueron descargados por Internet o por correo electrónico, deberán ser revisados por el antivirus inmediatamente después de haber sido desempaquetados y antes de ser ejecutados.

14. INTERCAMBIO DE INFORMACIÓN

- No estará permitido intercambiar información con entidades externas sin la debida autorización y/o acuerdos de confidencialidad que garantice los tratamientos de información pertinentes.
- Cuando se envíe información sensible por correo electrónico, se debe colocar clave a los archivos adjuntos y está debe ser informada al destinatario por un medio diferente al correo electrónico.
- Los empleados de la Cooperativa y de las empresas aliadas deben estar cubiertos con acuerdos de confidencialidad y, por lo tanto, serán responsables de la entrega de información no autorizada.
- En caso de ser necesario el envío y la recepción de información confidencial con los terceros contratados, se debe proteger con mecanismos de cifrado fuerte.
- La información sensible disponible al público a través de sitios web, debe estar protegida por sitios seguros y, adicionalmente, con usuario y clave de acceso.
- La comunicación con entidades externas para el intercambio de información crítica se debe hacer a través de canales dedicados, con mecanismos de seguridad, como son VPN o webservices y debe ser configurado por personal de la Cooperativa.
- Se debe emplear cifrado fuerte para la transmisión de la información, así mismo la Cooperativa evaluará con regularidad la efectividad y vigencia de los mecanismos de cifrado adoptados.
- Es responsabilidad de los dueños de la información crítica no dejar copias impresas o documentos físicos en lugares de fácil acceso a personal no autorizado.
- En los contratos o acuerdos de servicios se incluyen los requisitos y condiciones requeridas para el intercambio de información.

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

	PROCESO		GESTIÓN DE SISTEMAS					
	MANUAL		MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS					
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022	página	17 de 26

15. RESPALDO DE LA INFORMACIÓN

A toda la información que se encuentra alojada en los servidores y equipos de cómputo, se le debe garantizar respaldo periódicamente de acuerdo con los procedimientos establecidos, con el fin de contar con la información en caso de ser requerida por alguna eventualidad y se tendrá en cuenta que:

- Las copias de seguridad deben estar enfocadas a los datos, sistemas y programas, servidores, equipos de escritorio, portátiles, red, sistemas de control, sistemas de seguridad, entre otros.
- Debe garantizar que los medios de respaldo están físicamente protegidos / asegurados al menos al mismo nivel que los datos operacionales.
- Las copias de seguridad se deben almacenar en ubicaciones adecuadas, protegidos contra desastres físicos y acceso indebido.
- Se debe implementar un procedimiento para probar, de forma regular, las copias generadas y así garantizar su integridad y funcionalidad al momento de una restauración.

16. SINCRONIZACIÓN DE RELOJES

Todos los equipos tanto, servidores, switches, equipos de cómputo, circuito cerrado de cámaras de vigilancia - CCTV, y todos aquellos dispositivos tecnológicos que se tienen en la Cooperativa se deben sincronizar a la hora legal colombiana, sin excepción alguna. Se debe garantizar, por medio de seguimiento y con el respectivo indicador, el cumplimiento de la correcta sincronización de la hora según lo expuesto en el numeral 14, del artículo 6, del Decreto 4175 de 2011, con apoyo del Instituto Nacional de Metrología de Colombia (www.inm.gov.co, opción hora legal).

17. CONTROLES DE ACCESO

Se aplica a todas las formas de acceso a las instalaciones de la Cooperativa y para aquellas áreas definidas como “áreas críticas”, debido a su relación con datos confidenciales y de interés para el negocio, así:

- El acceso de todo el personal (incluyendo contratistas y visitantes) a los Datacenter y Centros de Cableado, debe estar restringido y sólo pueden acceder a través de la autorización del correspondiente funcionario.

 COOPEAIPÉ <small>Cooperativa de Ahorro y Crédito Empresa de Proyección Alpuna</small>	PROCESO		GESTIÓN DE SISTEMAS					
	MANUAL		MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS					
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022	pagina	18 de 26

- Para preservar la seguridad de los equipos de los servidores y equipos de comunicaciones y, en general, todos los dispositivos de los Datacenters, centros de cableado y los armarios (Racks), deben permanecer cerrados.
- Si se requiere el uso de cámaras de video (CCTV) u otros mecanismos de control de acceso (proximidad o control de acceso biométrico) para supervisar el acceso físico de personas a áreas críticas o que resguardan información confidencial, deben generar su respectivo procedimiento de tratamiento de copias de seguridad a menos que la ley u otras regulaciones requieran un tiempo superior de custodia.
- Se deben implementar controles físicos que impidan el acceso a conexiones o puntos de red de acceso público. Esto incluye limitar el acceso físico a los puntos de acceso inalámbricos, dispositivos de telecomunicaciones, manuales, hardware de redes o comunicaciones y líneas de telecomunicaciones.

18. TELETRABAJO

Teletrabajo significa que los equipos de información y comunicación se utilizan para permitir que los empleados realicen su trabajo fuera de la Cooperativa. Esto incluye el uso de teléfonos móviles, tabletas y similares fuera de las instalaciones de la Cooperativa, por lo cual:

- El acceso remoto a los servidores que se encuentran fuera de las instalaciones de la Cooperativa debe estar autorizado por el comité de riesgos o quien delegue la gerencia general.
- Las áreas de trabajo remoto que autorice la Cooperativa fuera de su sede principal deben cumplir con todas las políticas y controles del sistema de seguridad definido para proteger la información que viaje en ellos.
- El personal de infraestructura de informática y tecnología son responsables de proporcionar el servicio de acceso

19. ACCESO A LAS REDES WIFI

- El acceso a las redes inalámbricas por parte de los empleados, a través de WiFi, se debe realizar con autenticación usuario y contraseña.
- Las redes WiFi para asociados o visitantes se debe realizar mediante accesos independientes y por redes lógicas independientes a las redes corporativas.

 COOPEALPINE <i>Empresa de Proyección Alpina</i>	PROCESO		GESTIÓN DE SISTEMAS				
	MANUAL		MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022	página 19 de 26

20. ASPECTOS NO PERMITIDOS

Los aspectos no permitidos deben quedar contenidos en políticas, principios o procedimientos, manuales y ser de conocimiento por todos los funcionarios de la Cooperativa, entre ellos:

- Transmisión de contenido fraudulento, difamatorio, obsceno, ofensivo o de vandalismo, insultante o acosador, sea este material o mensajes.
- Interceptar, recopilar o almacenar datos sobre terceros sin su conocimiento o consentimiento.
- Escanear o probar la vulnerabilidad de equipos, sistemas o segmentos de red.
- Enviar mensajes no solicitados (spam), virus, o ataques internos o externos.
- Obtener acceso no autorizado a equipos, sistemas o programas, tanto al interior de la red como fuera de ella. Tampoco se podrá utilizar la red WIFI para obtener, manipular y compartir cualquier archivo de tipo musical o filmográfico, sin tener los derechos de propiedad intelectual.
- Dañar equipos, sistemas informáticos o redes y/o perturbar el normal funcionamiento de la red. Ser usada con fines de lucro, actividades comerciales o ilegales, por ejemplo, hacking. Ser utilizada para crear y/o la colocar un virus informático o programa maligno en la red.
- Transmitir, copiar y/o descargar cualquier material que viole cualquier ley. Esto incluye entre otros: material con derecho de autor, pornografía infantil, material amenazante u obsceno o material protegido por secreto comercial o patentes.

21. PRESTACIÓN DE SERVICIOS POR TERCERAS PARTES

Cuando la Cooperativa requiera la contratación de prestación de servicios por terceras partes debe, como mínimo:

- Firmar el documento de acuerdo de confidencialidad antes de iniciar la prestación del servicio.
- Elaborar los contratos o acuerdos de prestación de servicios donde se especifiquen claramente las condiciones.
- Cuando existan cambios en los servicios que prestan las terceras partes, estos deben ser documentados e incluidos en los acuerdos de servicios o contratos.
- La Cooperativa realizará auditorías a las terceras partes para evaluar la seguridad de la información y, como mínimo, se evaluarán integridad, disponibilidad, confidencialidad y calidad del servicio.

	PROCESO		GESTIÓN DE SISTEMAS					
	MANUAL		MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS					
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022	pagina	20 de 26

22. GESTIÓN DE INCIDENTES DE SEGURIDAD

Existen varias categorías de incidentes de seguridad que se pueden llegar a presentar, dentro de las cuales se encuentran:

22.1. Acceso no autorizado: Comprende todo tipo de ingreso y operación no autorizado a los sistemas, tanto exitosos como no exitosos. Son parte de esta categoría:

- Accesos no autorizados exitosos, sin perjuicios visibles a componentes tecnológicos.
- Robo de información
- Borrado de información
- Alteración de la información
- Intentos recurrentes y no recurrentes de acceso no autorizado
- Abuso y/o Mal uso de los servicios informáticos internos o externos que requieren autenticación

22.2. Código malicioso: Esta categoría comprende la introducción de códigos maliciosos en la infraestructura tecnológica de la Cooperativa. Son parte de esta categoría:

- Virus informáticos
- Troyanos
- Gusano informáticos

22.3. Denegación del servicio: Esta categoría incluye los eventos que ocasionan pérdida de un servicio en particular. Los síntomas para detectar un incidente de esta categoría son:

- Tiempos de respuesta muy bajos sin razones aparentes.
- Servicio(s) interno(s) inaccesibles sin razones aparentes
- Servicio(s) Externo(s) inaccesibles sin razones aparentes

22.4. Escaneos, pruebas o intentos de obtención de información de la red o de un servidor en particular. Esta categoría agrupa los eventos que buscan obtener información de la infraestructura tecnológica de la Cooperativa y comprende:

- Sniffers (software utilizado para capturar información que viaja por la red)
- Detección de Vulnerabilidades

	PROCESO		GESTIÓN DE SISTEMAS				
	MANUAL		MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022	página 21 de 26

22.5. Mal uso de los recursos tecnológicos: Esta categoría agrupa los eventos que atentan contra los recursos tecnológicos por el mal uso y comprende:

- Mal uso y/o Abuso de servicios informáticos internos o externos
- Violación de las normas de acceso a Internet
- Mal uso y/o Abuso del correo electrónico de la Cooperativa
- Violación de las Políticas, Normas y Procedimientos de Seguridad Informática establecidas para proteger la información

Es deber de la Cooperativa reportar un incidente de seguridad tan pronto lo detecte o se sospeche de él, aplicando el procedimiento interno definido para tal efecto. Adicionalmente, si estos desencadenan en fraudes para la Cooperativa se deberán poner en contacto con las entidades encargadas para la investigación y sanción de estos hechos denominados delitos informáticos, así como informar tal situación a la Superintendencia de la Economía Solidaria.

23. DIVULGACIÓN DE INFORMACIÓN

Diseñar procedimientos para dar a conocer a los asociados, usuarios y funcionarios, los riesgos derivados del uso de los diferentes medios y canales.

24. INVENTARIO DE ACTIVOS

La Cooperativa deberá contar con un inventario de activos de la información, especificando, como mínimo, los siguientes aspectos:

- Datos digitales
- Información impresa
- Software
- Infraestructura
- Servicios de información y proveedores de servicios
- Seguridad física
- Relaciones comerciales
- Responsables de los activos.

Se deben identificar los activos asociados con información e instalaciones de procesamiento de información. Así mismo, se deberá contar con un proceso y procedimiento detallado para mantener el inventario en una condición

 COOPEAIPÉ <small>Cooperativa de Ahorro y Crédito Empresa de Proyección Alpuna</small>	PROCESO		GESTIÓN DE SISTEMAS				
	MANUAL		MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022	pagina 22 de 26

razonablemente completa, precisa y actualizada a pesar de los cambios de equipo / personal, nuevos sistemas, negocios y cambios de TI.

25. POS (incluye PIN Pad)

La Cooperativa debe verificar que los POS cumplan, como mínimo, con los siguientes requerimientos:

- La lectura de tarjetas solo se deberá hacer a través de la lectora de los datáfonos y los PIN Pad cumpliendo con los estándares PCI-DSS.
- Los administradores de tecnología son los responsables de validar automáticamente la autenticación del datáfono que se intenta conectar a ellos, así como garantizar que los canales de comunicación se encuentren con los debidos controles criptográficos descritos en el presente documento.
- Establecer procedimientos que le permitan identificar los responsables de los datáfonos en los establecimientos comerciales y confirmar la identidad de los funcionarios autorizados para retirar o hacerles mantenimiento a los equipos.
- Velar porque la información confidencial de los asociados y usuarios no sea almacenada o retenida en el lugar en donde los POS estén siendo utilizados reduciendo la posibilidad que terceros puedan ver la clave digitada por el asociado o usuario.

26. TRANSACCIONES POR INTERNET

La Cooperativa deberá cumplir como mínimo lo siguiente:

- Implementar los controles descritos en los algoritmos y protocolos necesarios para brindar una comunicación segura.
- Realizar, como mínimo dos (2) veces al año, una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados en la realización de transacciones por este canal. Sin embargo, cuando se realicen cambios en la plataforma que afecten la seguridad del canal, deberá realizarse una prueba adicional, esto debe ir acompañado de su respectivo documento de control de cambios.
- Promover y poner a disposición de sus asociados mecanismos que reduzcan la posibilidad de que la información de sus transacciones pueda ser capturada por terceros no autorizados durante cada sesión.

 COOPEA IPE <small>Cooperativa de Ahorro y Crédito Empresa de Proyección Alpuna</small>	PROCESO		GESTIÓN DE SISTEMAS				
	MANUAL		MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022	página 23 de 26

- Establecer el tiempo máximo de inactividad, después del cual se deberá dar por cancelada la sesión, exigiendo un nuevo proceso de autenticación para realizar otras operaciones.
- Informar al asociado, al inicio de cada sesión, la fecha y hora del último ingreso a este canal.
- Implementar mecanismos que permitan a la Cooperativa verificar constantemente que no sean modificados los enlaces (links) de su sitio Web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS.

27. ANÁLISIS DE VULNERABILIDADES

La Cooperativa deberá implementar un sistema de análisis de vulnerabilidades informáticas que cumpla al menos con los siguientes aspectos:

- Estar basado en un hardware de propósito específico (appliance) totalmente separado e independiente de cualquier dispositivo de procesamiento de información, de comunicaciones y/o de seguridad informática.
- Generar, de manera automática, por lo menos dos (2) veces al año, un informe consolidado de las vulnerabilidades encontradas. Los informes de los últimos dos (2) años deben contener sus planes de acción y sus remediaciones.
- Realizar un análisis diferencial de vulnerabilidades, comparando el informe actual con respecto al inmediatamente anterior.
- Las herramientas usadas en el análisis de vulnerabilidades deberán estar homologadas por el CVE (Common Vulnerabilities and Exposures) y actualizadas a la fecha de su utilización.
- Los informes generados deberán tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre (www.mitre.org).

28. SEGURIDAD FÍSICA Y DEL ENTORNO.

La Cooperativa debe implementar una política para prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la Cooperativa. Para ello, la política debe contemplar, como mínimo:

- Estudio acerca de si las instalaciones se encuentran en una zona de riesgo.
- Se definen los perímetros de seguridad (edificios, oficinas, redes informáticas, habitaciones, armarios de red, archivos, salas de máquinas, etc.).

	PROCESO	GESTIÓN DE SISTEMAS				
	MANUAL	MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022

pagina 24 de 26

- Tipo de construcción, en la cual se ubican los activos informativos de la Cooperativa especificando la seguridad con la que cuentan el techo, el exterior, las paredes, el suelo, las ventanas, las puertas y cualquier acceso físico a la ubicación de los equipos que contienen la información.
- Controles físicos a todos los puntos de acceso externos adecuadamente protegidos contra el acceso no autorizado.
- Controles implementados a puertas y ventanas para determinar su nivel de seguridad ante algún tipo de intento de violación.
- Monitoreo a los puntos de acceso con cámaras.
- Pruebas programadas al sistema de detección de intrusos de la Cooperativa.

29. INSTALACIONES Y SUMINISTROS

La Cooperativa debe proteger los equipos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. Por lo tanto, deberá contar con lo siguiente:

- Un sistema de UPS para proporcionar una potencia adecuada, confiable y de alta calidad para abarcar todos los equipos esenciales durante un período de tiempo suficiente.
- Un plan de mantenimiento y pruebas para los UPS y generadores.
- Contar con una red de suministro eléctrico redundante
- Implementar controles para las pruebas de cambio y así garantizar la no afectación de los sistemas y servicios.
- Contar con sistemas de aire acondicionado redundantes para controlar entornos con equipos críticos y así mantener una capacidad adecuada de A/C para soportar la carga de calor.
- Implementar detectores de temperatura.

30. Planificación e implementación de la continuidad de la seguridad de la información

La Cooperativa 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. Así mismo, deberá establecer, documentar, implementar y mantener procesos procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información.

	PROCESO		GESTIÓN DE SISTEMAS					
	MANUAL		MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS					
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022	pagina	25 de 26

De igual forma, la Cooperativa 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. Por lo tanto, deberá contemplar los siguientes aspectos fundamentales:

- Determinar los requisitos de continuidad del negocio.
- Elaborar un plan de continuidad de negocio.
- Contar con un diseño adecuado de "alta disponibilidad" para sistemas de TI, redes y procesos críticos.
- Identificar el impacto potencial de los incidentes.
- Evaluar los planes de continuidad del negocio.
- Realizar DRP para validar el nivel de respuesta de la Cooperativa ante un incidente.
- Los planes deberán tener plazos definidos para restaurar servicios tras una interrupción.
- Los planes deberán contar con la identificación y asignación de responsabilidades, la identificación de pérdidas aceptables, la implementación de procedimientos de recuperación y restauración, la documentación de procedimientos y las pruebas regulares.
- La planificación de la continuidad deberá ser consistente y debe identificar las prioridades de restauración.
- Deberá contar con miembros de los equipos de recuperación o gestión de crisis o incidentes, con conocimiento de los planes, estableciendo de forma clara sus roles y responsabilidades.
- Los controles de seguridad deberán estar adecuados para los sitios de recuperación de desastres remotos.
- Deberá contar con un método de pruebas del plan de continuidad.
- Se debe establecer la frecuencia con la que se lleven a cabo las pruebas.
- Deberán llevar un registro de evidencias de las pruebas reales efectuadas, junto con sus resultados y planes de mejora.
- Deberán identificar deficiencias para así remediarlas y posteriormente volverlas a probar hasta que los resultados sean satisfactorios.

31. REUTILIZACIÓN O ELIMINACIÓN SEGURA DE EQUIPOS

La Cooperativa debe implementar una política para establecer controles con el propósito de verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reuso.

La versión vigente y controlada de este documento, solo podrá ser consultada a través del espacio virtual o espacio físico definido por el área de procesos o quien haga sus veces. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la entidad.

	PROCESO	GESTIÓN DE SISTEMAS				
	MANUAL	MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS				
	Código	SI-MA-1	Versión	1	Emisión	marzo/2022
		página	26 de 26			

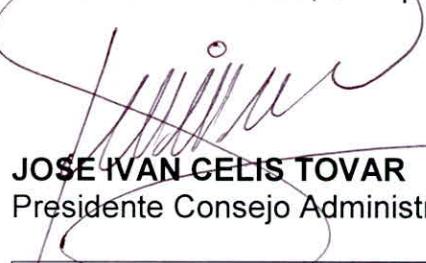
- La Cooperativa debe evitar que se revele la información almacenada en equipos y dispositivos tras su reasignación o eliminación, mediante el uso de cifrado fuerte o borrado seguro.
- Llevar un control y registro de cada uno de los medios que se eliminan.

El **MANUAL DE LA SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS**, será revisado y actualizado con la regularidad que se requiera, teniendo en cuenta las reglamentaciones expedidas y las necesidades propias de **COOPEAYPE**

El presente manual entrará en vigor a partir de su aprobación por parte del Consejo de Administración y publicación respectiva; deroga todas las disposiciones anteriores y todas aquellas normas que le sean contrarias.

Comuníquese y Cúmplase,

En constancia firman, en Aipe - Huila a los 02 días del mes de abril del año 2022.


JOSE IVAN CELIS TOVAR
Presidente Consejo Administración


AGUSTIN CHARRY CHARRY
Secretario Consejo Administración

Control de Cambios	
Versión	Observación
1	Aprobación inicial ACUERDO No 38 de abril de 2022

El presente Manual, fue socializado y aprobado por el Consejo de Administración, en uso de sus facultades legales, estatutarias y reglamentarias, en reunión del día 02 del mes abril del año 2022, y según consta en el acta extraordinaria de consejo de administración número 07.