RESOLUCIÓN NO. SEPS-IGS- IGT-IGJ-INGINT-INTIC-INSESF-INR-DNSI 2022-002

"Norma de control respecto a la seguridad de la Información en las entidades del sector financiero popular y solidario bajo el control de la Superintendencia de Economía Popular y Solidaria"

CONTENIDO

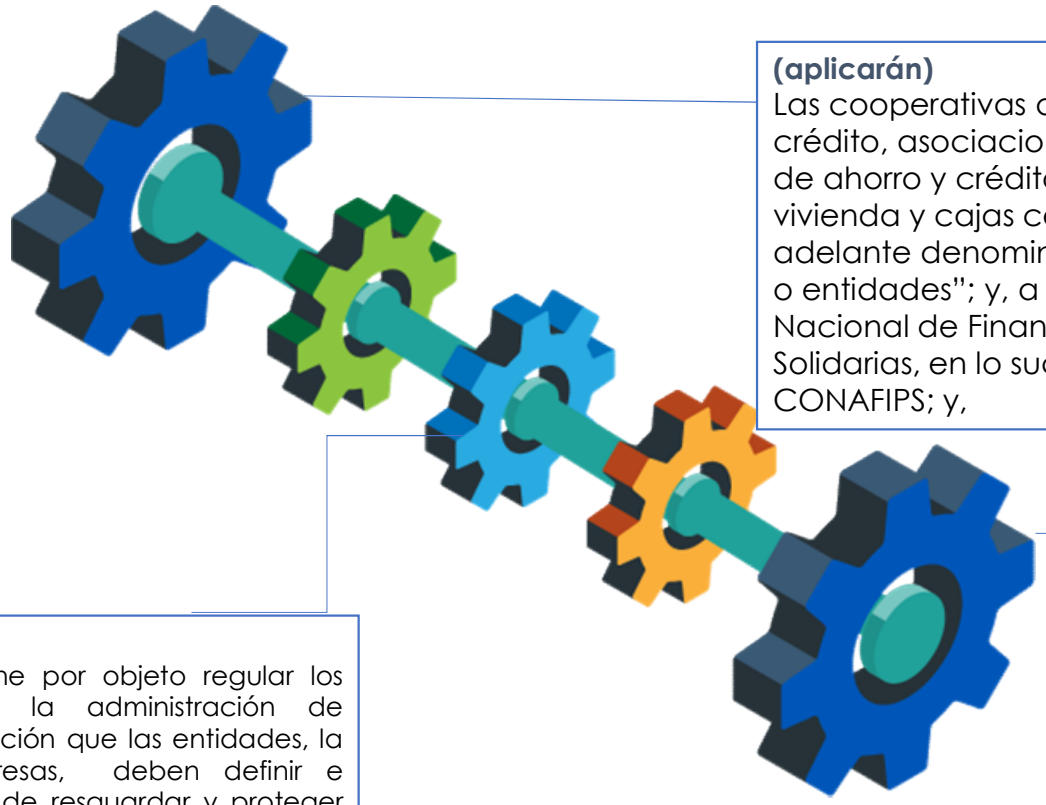
1. Objetivos, ámbito, y definiciones
2. Regímenes
3. Disposiciones transitorias
4. Controles Obligatorios

1 ÁMBITO, OBJETO, DEFINICIONES

OBJETO - ÁMBITO

ÁMBITO

OBJETO



(aplicarán)
Las cooperativas de ahorro y crédito, asociaciones mutualistas de ahorro y crédito para la vivienda y cajas centrales, en adelante denominadas "entidad o entidades"; y, a la Corporación Nacional de Finanzas Populares y Solidarias, en lo sucesivo CONAFIPS; y,

OBJETO
La presente norma tiene por objeto regular los niveles mínimos para la administración de seguridad de la información que las entidades, la CONAFIPS y las empresas, deben definir e implementar con el fin de resguardar y proteger sus activos de información, preservando su confidencialidad, disponibilidad e integridad.

Las compañías y organizaciones de servicios auxiliares que prestan servicios a las actividades financieras de las entidades y CONAFIPS, en adelante "empresas".

DEFINICIONES

DEFINICIONES– SEPS

- **NORMA DE CONTROL RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN EN LAS ENTIDADES DEL SECTOR FINANCIERO POPULAR Y SOLIDARIO BAJO CONTROL DE LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA**l.

Activo de información: Se consideran a los servicios o herramientas creados o utilizados en medios digital, físico, electromagnético y otros; hardware o software, utilizados para el procesamiento, transferencia o almacenamiento de información; y, cualquier dato que tenga información valorada por la entidad, CONAFIPS o empresa.

Bitácora de eventos de riesgos: Registro de eventos de riesgo durante un periodo en particular. Se registrará acorde a la "Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del Sector Financiero Popular y Solidario bajo el control de la Superintendencia de Economía Popular y Solidaria.

Partes interesadas: Son todas las personas naturales o jurídicas que, de alguna forma, puedan verse afectadas por la actividad de la entidad, de la CONAFIPS o de la empresa

2

REGÍMENES

Regímenes

Para efectos de esta norma, se aplicarán los siguientes regímenes

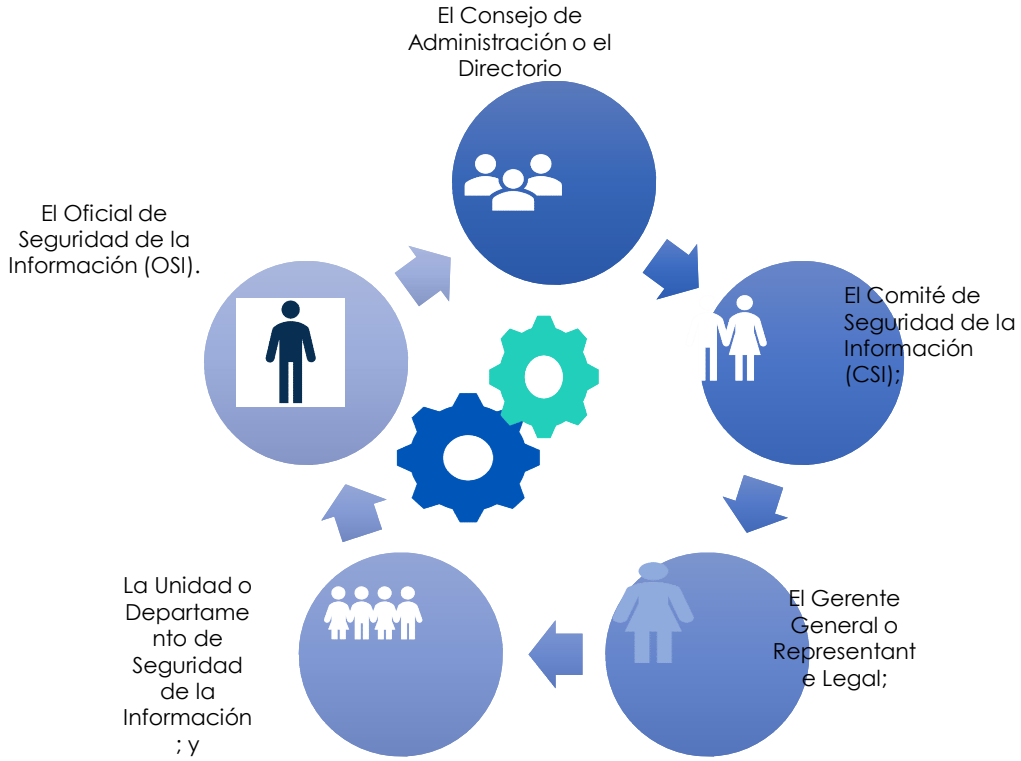
- A las cooperativas de ahorro y crédito de los segmentos 1 y 2; a las asociaciones mutualistas de ahorro y crédito para la vivienda y a la CONAFIPS;
- A las cooperativas de ahorro y crédito del segmento 3; y
- A las cooperativas de ahorro y crédito de los segmentos 4 y 5.

A las empresas se aplicarán los regímenes anteriores según el tipo de servicio que presten, de acuerdo con la siguiente tabla:

Tipos de Servicios Auxiliares	General	Especial	Simplificado
Software financiero y computación	x		
Transaccionales y de pago	x		
Transporte de especies monetarias y de valores		x	
Red de cajeros automáticos	x		
Cobranzas		x	
Generadoras de cartera	x		
Administradoras de tarjetas	x		
Giro inmobiliario			x
Servicios contables			x

SEGURIDAD DE LA INFORMACIÓN – RÉGIMEN GENERAL

RÉGIMEN GENERAL: CONFORMACIÓN



Comité de Seguridad de la Información (CSI)

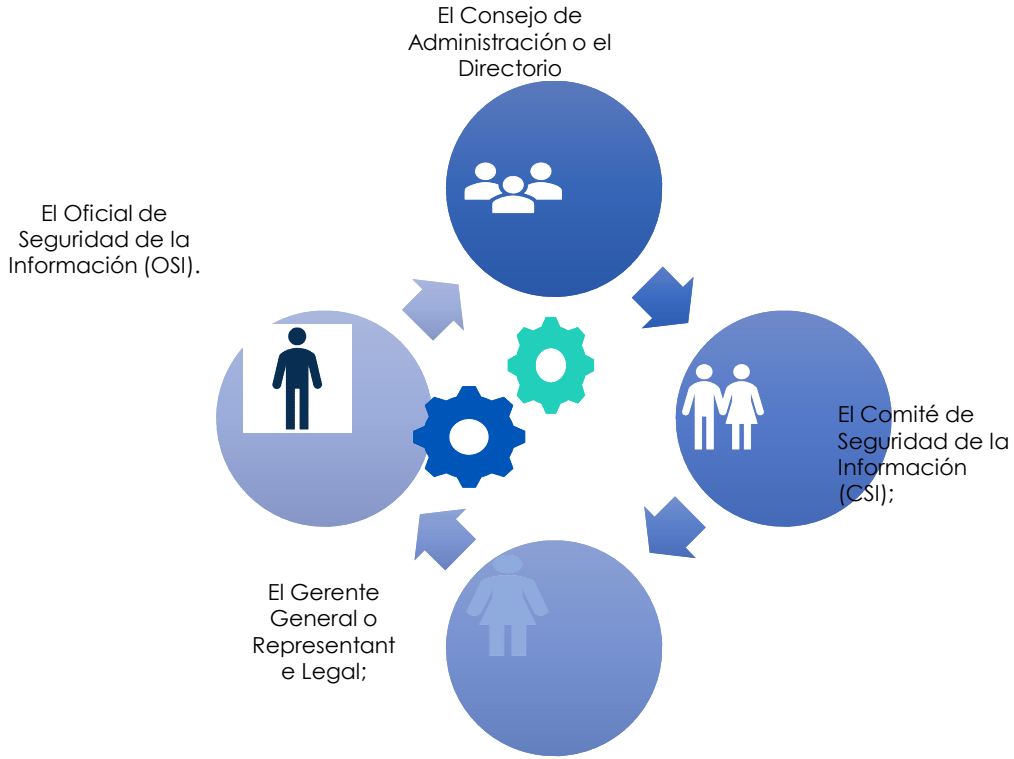
Las entidades, empresas y la CONAFIPS que conforman este régimen, deberán contar con un Comité de Seguridad de la Información (CSI), conformado por los siguientes miembros:

a) El presidente del Comité de Administración Integral de Riesgos, quien presidirá también el Comité de Seguridad de la Información y tendrá voto dirimente;
b) El Gerente General o representante legal;
c) El oficial de seguridad de la información, quien actuará como secretario del Comité;
d) El responsable del área de tecnología o su delegado; y,
e) Un delegado de Auditoría Interna.

El Comité podrá invitar a las sesiones a los responsables de las áreas de negocio que juzgue del caso, quienes tendrán voz pero no voto.

SEGURIDAD DE LA INFORMACIÓN – RÉGIMEN ESPECIAL

RÉGIMEN ESPECIAL: CONFORMACIÓN



Comité de Seguridad de la Información (CSI)

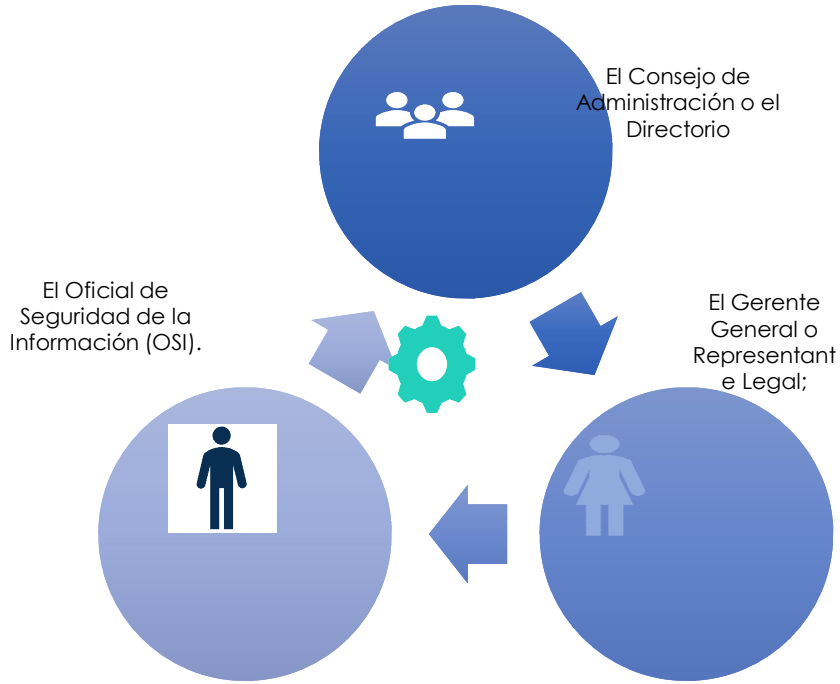
Las entidades y empresas que conforman este régimen, deberán contar con un Comité de Seguridad de la Información (CSI), conformado por los siguientes miembros:

- El presidente del Comité de Administración Integral de Riesgos, quien presidirá también el Comité de Seguridad de la Información y tendrá voto dirimente;
- El Gerente General o representante legal;
- El oficial de seguridad de la información, quien actuará como secretario del Comité;
- El responsable del área de tecnología o su delegado; y,
- Un delegado de Auditoría Interna.

El Comité podrá invitar a las sesiones a los responsables de las áreas de negocio que juzgue del caso, quienes tendrán voz pero no voto.

SEGURIDAD DE LA INFORMACIÓN – RÉGIMEN SIMPLIFICADO

RÉGIMEN SIMPLIFICADO: CONFORMACIÓN



Requisitos obligatorios para el Régimen Simplificado.

Las entidades y empresas pertenecientes a este régimen deberán contar con al menos, lo siguiente:
Políticas, procesos, procedimientos, roles y responsabilidades para la gestión de seguridad de la información;
Asignación de recursos humanos, técnicos y financieros para seguridad de la información;
Actividades de concienciación y formación en temas concernientes en seguridad de la información;
Los requerimientos señalados en el Anexo 1 de esta resolución, correspondiente al Régimen Simplificado; y,
Registro de los eventos relacionados con seguridad de la información en la "Bitácora de Eventos de Riesgos", para lo cual podrán basarse en la metodología de riesgos que se adjunta en el Anexo 2.

3

DISPOSICIONES GENERALES Y TRANSITORIAS

GENERALES

Las entidades, empresas y CONAFIPS, sin perjuicio de la información que solicite en cualquier momento este Organismo de Control, deberán reportar a la Superintendencia de Economía Popular y Solidaria, de forma inmediata, los eventos que afecten directamente a la continuidad del negocio y a la prestación de servicios financieros, incluyendo al menos la fecha del incidente, el impacto, el/los sistemas o servicios, y/o actividades afectadas, en la forma y medios que esta Superintendencia establezca para el efecto.

Las entidades, empresas y CONAFIPS deberán solicitar al menos una vez al año a los prestadores de servicios, sean estos personas naturales o jurídicas, la documentación que demuestre que el servicio prestado cuenta con las revisiones (auditorías, exámenes especiales, certificaciones, entre otros) y controles necesarios para una adecuada administración de la seguridad de la información.

TRANSITORIAS

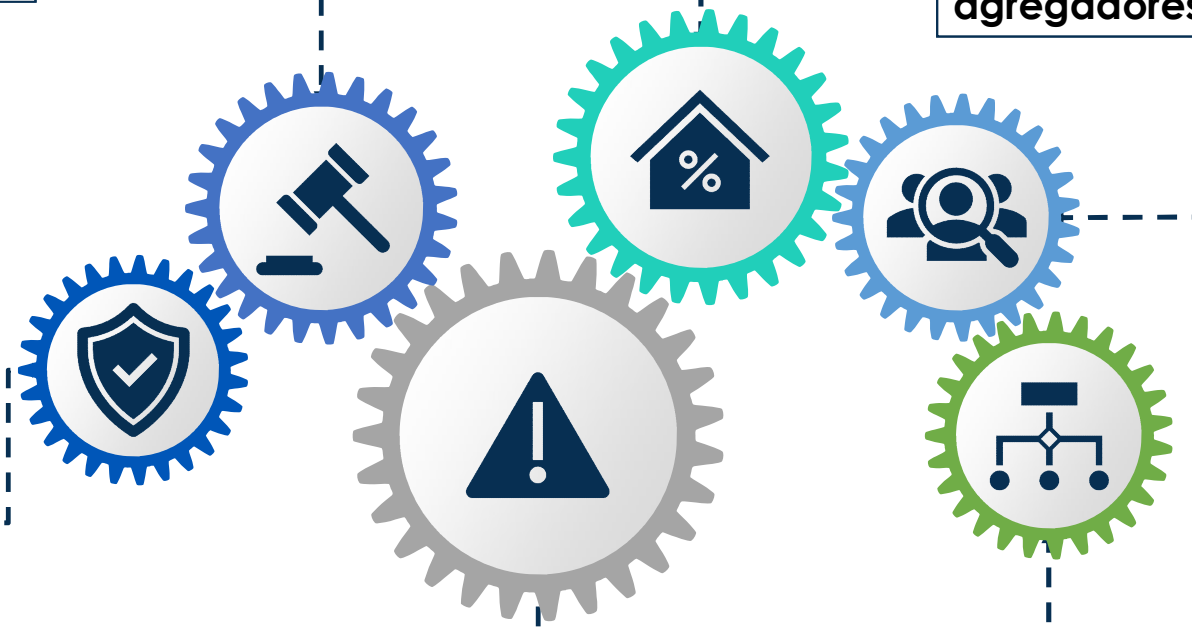
SEGMENTO	PLAZOS
SEGMENTO 1	12 meses
SEGMENTO 2	24 meses
SEGMENTO 3	36 meses
SEGMENTO 4 y **5**	24 meses
Cajas Centrales	12 meses
Asociaciones Mutualistas de ahorro y crédito para la vivienda	12 meses
CONAFIPS	12 meses
Compañías y Organizaciones de servicios auxiliares	24 meses

El primer oficial de seguridad de la información y el primer responsable de seguridad de la información, según corresponda, podrán acreditar el cumplimiento de los requisitos de capacitación previstos en esta norma, dentro del plazo de 6 meses contados a partir de su designación o contratación. La Superintendencia, en casos debidamente justificados y aceptados por este Organismo de Control, podrá ampliar dicho plazo por una sola vez

4

CONTROLES OBLIGATORIOS

CONTROLES



- Políticas
- Identificación de procesos agregadores de valor
- Clasificación de información
- Auditorías
- Respaldos
- Gestión de riesgos

GRACIAS POR SU ATENCIÓN

10 AÑOS
SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

www.seps.gob.ec
https://estadisticas.seps.gob.ec
https://data.seps.gob.ec

Matriz: Av. Amazonas N32-87 y La Granja / **PBX**: (593 2) 394 8840

@SEPS_Ec @sepsecuador Seps_ec sepsecuador