SUSEP
SUPERINTENDÊNCIA DE SEGUROS PRIVADOS

MANUAL DE ORIENTAÇÕES SOBRE SEGURANÇA CIBERNÉTICA

MANUAL DE ORIENTAÇÕES SOBRE SEGURANÇA CIBERNÉTICA

DIRETORIA DE REGULAÇÃO PRUDENCIAL E ESTUDOS ECONÔMICOS – DIRPE
Coordenação-Geral de Regulação Prudencial e Contábil – CGPEC
Coordenação de Regulação de Gestão de Riscos e de Ativos – COGRA

DIRETORIA DE SUPERVISÃO PRUDENCIAL E DE RESSEGUROS – DISUP
Coordenação-Geral de Supervisão Consolidada – CGCON
Coordenação de Supervisão Consolidada 4 – CONS4

Vigência: a partir de junho/2026
Versão: junho/2026

Sumário

1. INTRODUÇÃO

1.1 Áreas Responsáveis

Unidade	Competência
DIRPE/CGPEC cgpec@susep.gov.br **DIRPE/CGPEC/COGRA** cogra@susep.gov.br	Compete à Coordenação Geral de Regulação Prudencial e Contábil (CGPEC), e em especial à sua Coordenação de Regulação de Gestão de Riscos e de Ativos (COGRA), a regulação do tema segurança cibernética.
DISUP/CGCON cgcon@susep.gov.br **DISUP/CGCON/CONS4** cons4@susep.gov.br	Compete à Coordenação Geral de Supervisão Consolidada (CGCON), e em especial à sua Coordenação de Supervisão Consolidada 4 (CONS4), a supervisão quanto ao cumprimento de normas e padrões relativos ao tema segurança cibernética.

1.2 Base Legal

- ✓ Resolução CNSP nº 416, de 20 de julho de 2021;
- ✓ Resolução CNSP nº 491 de 04 de Maio de 2026;
- ✓ Resolução CNSP nº 492 de 04 de Maio de 2026;
- ✓ Circular Susep nº 638, de 27 de julho de 2021; e
- ✓ Circular Susep nº 700, de 4 de abril de 2024.

1.3 Abrangência

- ✓ seguradoras;
- ✓ entidades abertas de previdência complementar (EAPCs);
- ✓ sociedades de capitalização;
- ✓ resseguradores locais;
- ✓ sociedades cooperativas de seguros; e
- ✓ administradora de operações de proteção patrimonial mutualista.

Ao longo deste Manual, as entidades e sociedades acima são tratadas como supervisionadas.

1.4 Objetivo

O presente documento tem por objetivo orientar as supervisionadas quanto à implementação dos requisitos mínimos de segurança cibernética previstos na Circular Susep nº 638, de 2021, e na Resolução CNSP nº 491, de 2026, combinadas com as demais normas correlatas, Resoluções CNSP nº 416, de 2021, e nº 492, de 2026, e Circular Susep nº 700, de 2024.

Adicionalmente, são apresentados como destaque e denominado como "BOAS PRÁTICAS", pontos de atenção evidenciados pela supervisão e que aqui são apresentados como recomendações, condutas desejáveis ou procedimentos mais eficazes a serem observados pelas supervisionadas.

2. CONCEITOS-CHAVE

2.1 Segurança Cibernética

Para fins regulatórios, a segurança cibernética corresponde ao conjunto de estratégias, políticas, padrões, processos, procedimentos e controles voltados à **mitigação do risco cibernético**, de modo a **garantir a resiliência operacional**, assegurando a continuidade das atividades consideradas críticas pelas supervisionadas, com a recuperação de incidentes cibernéticos em tempo adequado e com impactos controlados, visando a preservação da **confiabilidade** das informações, sistemas e serviços.

A **confiabilidade** compreende as seguintes dimensões:

- ✓ **confidencialidade das informações** - garantia de que a informação não seja disponibilizada ou divulgada a indivíduos, entidades ou processos não autorizados;
- ✓ **integridade dos dados e sistemas** - salvaguarda da exatidão e completude dos dados e sistemas; e
- ✓ **disponibilidade dos serviços e informações** - garantia de que usuários autorizados tenham acesso oportuno e confiável aos dados e serviços.

Embora eventos disruptivos sejam inerentes à operação, a resiliência cibernética das supervisionadas não deve se limitar à prevenção de riscos, devendo também priorizar a capacidade de absorver, resistir e se recuperar de incidentes, de modo a assegurar a continuidade dos serviços essenciais, mesmo sob condições adversas.

2.2 Risco Cibernético

Risco cibernético é a possibilidade de ocorrência de perdas resultantes do comprometimento da **confidencialidade, integridade ou disponibilidade** de dados e informações em suporte digital, em decorrência da sua manipulação indevida ou de danos a equipamentos e sistemas utilizados para seu armazenamento, processamento ou transmissão.

2.3 Serviços Relevantes

São serviços (incluindo nuvem e terceirizados) cuja indisponibilidade ou violação possa comprometer a continuidade de atividades que **a supervisionada considere** essencial para manutenção do seu negócio ou a confiabilidade de dados relevantes, compreendendo o acesso ou manipulação de dados, pessoais e relativos a clientes, e a processos críticos de negócios ou dados e informações considerados sensíveis pela própria supervisionada.

2.4 Incidentes Relevantes

Incidentes Relevantes são eventos disruptivos, originados ou não por ações maliciosas, que comprometem efetivamente a confidencialidade, integridade ou disponibilidade de sistemas, serviços ou dados relevantes. Diferenciam-se de eventos rotineiros por causarem um comprometimento substancial ou a interrupção de atividades e operações críticas, afetando a entrega de serviços aos segurados e a estabilidade operacional da instituição.

A Gestão de Incidentes é o componente crítico da resiliência operacional que gerencia o ciclo de vida completo de eventos disruptivos, integrando a prevenção proativa de vulnerabilidades à detecção e resposta tempestiva de incidentes. Ela deve atuar de forma coordenada para mitigar perdas resultantes do comprometimento da segurança digital, priorizando a recuperação ágil da infraestrutura e a proteção de dados relevantes, com vistas a assegurar a estabilidade das operações e a confiança das partes interessadas no ecossistema de seguros.

3. INSTRUÇÕES

3.1 Requisitos Gerais

Na adoção de tratamentos e controles destinados à mitigação dos riscos cibernéticos, devem ser observadas as boas práticas nacionais e internacionais de segurança cibernética, no mínimo no que se refere aos seguintes aspectos:

- ✓ segurança física de equipamentos, ativos e instalações;
- ✓ controle de acesso a sistemas, aplicações e informações;
- ✓ uso de mecanismos de criptografia compatíveis com o nível de sensibilidade das informações;
- ✓ proteção contra softwares maliciosos;
- ✓ realização e manutenção de cópias de segurança (*backup*) de dados e informações;
- ✓ manutenção de registros (*logs*) de atividades de usuários, bem como de exceções e falhas de sistemas;
- ✓ adoção de técnicas de proteção de redes e de segurança das comunicações; e
- ✓ desenvolvimento, aquisição e manutenção de sistemas de informação, observando requisitos de segurança desde a sua concepção.

Adicionalmente, devem ser promovidas ações voltadas à disseminação da cultura de segurança cibernética, incluindo a implementação de programa contínuo de capacitação e

conscientização dos colaboradores, compatível com a natureza e o grau de sensibilidade das informações por eles manipuladas.

3.2 Etapas da Implementação

PASSO 1. COMPREENDER O PAPEL DA SEGURANÇA CIBERNÉTICA

A segurança cibernética integra a gestão de riscos operacionais e deve ser tratada como tema de governança corporativa.

A regulamentação vigente estabelece requisitos mínimos para:

- ✓ proteger dados e informações relevantes;
- ✓ assegurar a continuidade dos serviços essenciais; e
- ✓ reduzir riscos operacionais no mercado supervisionado.

PASSO 2. INTEGRAR A SEGURANÇA CIBERNÉTICA AO GERENCIAMENTO DE RISCOS

A segurança cibernética deve estar integrada ao **Sistema de Controles Internos** (SCI) e à **Estrutura de Gestão de Riscos** (EGR), conforme regulamentação vigente.

A segurança cibernética deve ser compreendida como parte integrante do SCI e da EGR da supervisionada, e não como um tema isolado ou apenas tecnológico. Para facilitar a compreensão, as boas práticas ao longo do texto são apresentadas em quadros destacados na cor azul.

PASSO 3. ELABORAR E MANTER A POLÍTICA DE SEGURANÇA CIBERNÉTICA

As supervisionadas devem manter Política de Segurança Cibernética, aprovada pelos órgãos de administração, que estabeleça, no mínimo:

- ✓ os objetivos de segurança cibernética;
- ✓ o compromisso dos órgãos de administração com a segurança cibernética e com a melhoria contínua dos processos, procedimentos e controles a ela relacionados;
- ✓ os critérios de classificação de dados, serviços, incidentes e vulnerabilidades;
- ✓ as diretrizes para implementação de processos, procedimentos e controles de segurança; e
- ✓ regras para terceirização e computação em nuvem.

A Política de Segurança Cibernética deve ser compatível com o porte, a complexidade, o modelo de negócio e o perfil de risco da supervisionada, nos termos da regulamentação vigente. Essa política deve ser revisada sempre que houver alterações relevantes nesses elementos e, adicionalmente, de forma periódica, no mínimo anualmente, observando-se sua integração ao plano de negócios, do qual constitui parte integrante, nos termos do art. 61 da Circular Susep nº 700, de 2024.

Boa Prática:

Recomenda-se que a Política de Segurança Cibernética seja estruturada a partir de **critérios claros e objetivos para a classificação de dados, incidentes e serviços relevantes**, de modo a favorecer o alinhamento explícito entre essas classificações, os controles de segurança adotados e as diretrizes aplicáveis à terceirização, especialmente no caso de serviços relevantes.

Nesse contexto, é recomendável que as **diretrizes relativas à terceirização e à computação em nuvem** estejam incorporadas à Política de Segurança Cibernética, ainda que possam ser detalhadas em regramentos específicos, assegurando referência expressa, coerência e articulação entre os documentos. Essa integração contribui para o fortalecimento da governança e para a consistência do arcabouço de segurança cibernética.

PASSO 4. IDENTIFICAR E CLASSIFICAR DADOS RELEVANTES

Dados relevantes são aqueles que compreendem **dados pessoais**, conforme definidos na legislação em vigor, **dados relativos a clientes, informações vinculadas a processos críticos de negócio**, bem como **quaisquer outros dados ou informações consideradas sensíveis**, de acordo com as diretrizes estabelecidas pela própria supervisionada.

Cabe às **supervisionadas identificar e classificar os dados considerados relevantes**, incluindo, entre outros, os dados pessoais, os dados de clientes, as informações relacionadas a processos críticos de negócio e outros dados sensíveis por elas definidos.

PASSO 5. IDENTIFICAR ATIVIDADES ESSENCIAIS PARA CONTINUIDADE DO NEGÓCIO

As supervisionadas devem identificar **quais atividades são essenciais para continuidade do seu negócio**. Essas atividades devem compor o seu **núcleo operacional e estratégico**.

Pode-se destacar como principais candidatas, dentre outras, as seguintes atividades:

- ✓ **Subscrição de riscos**: O processo de aceitação e precificação dos riscos que a supervisionada assume;
- ✓ **Regulação de sinistros e concessão de benefícios**: O processamento, análise e pagamento de indenizações aos segurados, benefícios aos beneficiários ou prêmios aos detentores de títulos de capitalização;
- ✓ **Definição de provisões técnicas, prêmios e contribuições**: atividades atuariais que garantem a solvência e a capacidade financeira da supervisionada para honrar compromissos futuros;
- ✓ **Comercialização de produtos e planos**: as atividades de venda e distribuição de seguros e planos de previdência ou capitalização;
- ✓ **Realização de investimentos**: a gestão dos ativos financeiros da supervisionadas,

fundamentais para garantir as reservas técnicas; e

✓ **Cessão de riscos**: operações de **resseguro, cosseguro ou retrocessão**, essenciais para a pulverização do risco da carteira.

Importante destacar que uma atividade é considerada essencial se sua interrupção puder causar grave impacto operacional, tais como:

✓ **Danos substanciais à operação**: impacto na capacidade de prestar serviços ou cumprir obrigações contratuais;

✓ **Risco de liquidez**: a impossibilidade de a supervisionada cumprir eficientemente suas obrigações financeiras quando forem devidas; e

✓ **Comprometimento de dados relevantes**: quando a interrupção afeta o acesso ou a manipulação de dados de clientes ou processos críticos.

Portanto, em uma supervisionada, qualquer serviço (como armazenamento em nuvem ou processamento de dados) que dê suporte direto a processos críticos de negócios, **cuja descontinuidade cause grave impacto operacional**, deve ser classificado como essencial e aquele serviço como uma atividade essencial para continuidade do negócio.

PASSO 6. IDENTIFICAR SERVIÇOS RELEVANTES, INCLUSIVE EM NUVEM

Devem ser identificados os **serviços relevantes**, entendidos como aqueles que:

✓ envolvam acesso ou manipulação de **dados relevantes**; ou

✓ sejam **essenciais para a continuidade das atividades da supervisionada**, inclusive serviços terceirizados e de computação em nuvem.

Exemplos:

✓ Processamento, armazenamento e análise de dados, inclusive por meio de soluções baseadas em inteligência artificial;

✓ Serviços de segurança cibernética, incluindo monitoramento e detecção de ameaças, bem como testes e avaliações de segurança;

✓ Gestão de identidades e acessos (*Identity and Access Management – IAM*);

✓ Serviços de infraestrutura tecnológica, incluindo ambientes em nuvem;

✓ Serviços de gestão de riscos; e

✓ Serviços de continuidade de negócios.

A relação de serviços apresentada possui caráter **exemplificativo e não exaustivo ou taxativo**. **Cabe às supervisionadas identificar e definir quais serviços devem ser considerados relevantes** a partir de avaliação própria, baseada na mensuração do risco à segurança cibernética, observadas a natureza, a criticidade e o impacto potencial desses serviços sobre suas operações, ativos de informação e processos críticos de negócio.

PASSO 7. PREVENIR VULNERABILIDADES DE FORMA CONTÍNUA

As supervisionadas devem adotar abordagem preventiva e contínua, contemplando:

✓ identificação de vulnerabilidades técnicas, operacionais e organizacionais;

✓ correção tempestiva dessas vulnerabilidades; e

✓ monitoramento contínuo de sistemas e redes.

Boa Prática:

Recomenda-se a adoção de uma abordagem **preventiva e contínua** para a identificação e o tratamento de vulnerabilidades, de forma independente da ocorrência de incidentes.

Em consonância com a regulamentação vigente, é recomendável que as vulnerabilidades sejam **identificadas, registradas e tratadas de maneira sistemática e tempestiva**, no âmbito de um processo estruturado de gestão da segurança cibernética, contribuindo para a redução de riscos e para o fortalecimento da resiliência operacional.

PASSO 8. ESTABELECER PROCEDIMENTOS DE RESPOSTA A INCIDENTES

Devem existir procedimentos estruturados para:

- ✓ detecção de incidentes cibernéticos;
- ✓ implementar medidas de contenção;
- ✓ incluir, sempre que pertinente, comunicação prévia com prestadores de serviços, parceiros e outras partes potencialmente envolvidas;
- ✓ mitigação de impactos; e
- ✓ adotar uma resposta coordenada para recuperação segura dos serviços afetados.

Incidentes cibernéticos incluem eventos decorrentes ou não de ação maliciosa que comprometam dados ou sistemas digitais. A supervisionada deverá comunicar à Susep, no prazo máximo de 5 (cinco) dias úteis, a partir do conhecimento do evento, a ocorrência de incidentes relevantes, detalhando a extensão do dano causado e, se for o caso, as ações em curso para regularização completa da situação e os respectivos responsáveis e prazos.

Boa Prática:

Recomenda-se a adoção de uma **abordagem integrada** entre os processos de tratamento de incidentes e de gestão de vulnerabilidades, de modo a favorecer a adequada identificação das **causas raiz** e a implementação de **medidas preventivas** eficazes.

Nesse sentido, é recomendável que os incidentes sejam sistematicamente correlacionados às **vulnerabilidades** exploradas, possibilitando o fortalecimento dos controles existentes e promovendo o **aprimoramento contínuo** do arcabouço de segurança cibernética.

PASSO 9. INTEGRAR A SEGURANÇA CIBERNÉTICA AO PLANO DE CONTINUIDADE DE NEGÓCIOS

Ataques cibernéticos e falhas relevantes devem estar contemplados no **Plano de Continuidade de Negócios – PCN**, que deve assegurar:

- ✓ a manutenção ou retomada de processos críticos;
- ✓ a proteção de dados relevantes; e
- ✓ o retorno seguro às operações normais.

O plano deve ser testado periodicamente e revisado sempre que necessário, de forma a assegurar sua efetividade diante das ameaças de ataques cibernéticos.

Boa Prática:

Recomenda-se que o Plano de Continuidade de Negócios – PCN adote uma **abordagem abrangente**, contemplando não apenas cenários de indisponibilidade de sistemas, mas também situações associadas ao comprometimento de dados e à continuidade de serviços relevantes.

Nesse contexto, é recomendável que o PCN explicite, de maneira clara, cenários que envolvam, entre outros aspectos:

- ✓ danos a infraestruturas críticas de tecnologia da informação;
- ✓ acesso, modificação, exclusão ou divulgação não autorizados de dados relevantes; e
- ✓ interrupção de serviços relevantes.

A explicitação desses cenários contribui para o **aumento da robustez, da efetividade e da capacidade de resposta dos planos de continuidade**, fortalecendo a resiliência operacional da organização.

PASSO 10. GERIR ADEQUADAMENTE A TERCEIRIZAÇÃO E A COMPUTAÇÃO EM NUVEM

A contratação de terceiros ou serviços em nuvem **não transfere a responsabilidade** da supervisionada.

A regulação vigente prevê, entre outros aspectos:

- ✓ avaliação prévia da capacidade dos prestadores;
- ✓ definição de requisitos mínimos de segurança;
- ✓ garantia de acesso da Susep às informações, quando solicitado; e
- ✓ estratégias de substituição do prestador em caso de descontinuidade.

Boa Prática:

Recomenda-se que a gestão de terceiros adote uma abordagem que vá além dos aspectos estritamente contratuais, incorporando **mecanismos contínuos de acompanhamento e monitoramento dos serviços terceirizados**, especialmente sob a perspectiva da segurança da informação e da continuidade operacional.

Nesse sentido, é recomendável que a gestão de terceiros esteja **integrada à estrutura de gestão de riscos e à Política de Segurança Cibernética**, considerando que a terceirização não afasta a responsabilidade da instituição quanto à segurança e à continuidade dos serviços prestados.

PASSO 11. ELABORAR O RELATÓRIO ANUAL E FORTALECER A GOVERNANÇA

As supervisionadas devem elaborar **relatório anual** sobre prevenção e tratamento de incidentes e vulnerabilidades, contendo:

- ✓ análise dos incidentes relevantes;
- ✓ principais vulnerabilidades identificadas;
- ✓ ações corretivas adotadas ou planejadas;
- ✓ dados estatísticos consolidados; e
- ✓ resultados dos testes do PCN.

Esse relatório anual apoia: **a governança interna, a transparência e a melhoria contínua da gestão de riscos**.

Boa Prática:

Recomenda-se que o relatório anual de segurança cibernética apresente uma **visão abrangente e integrada dos principais eventos e riscos observados ao longo do período**, não se restringindo à descrição de incidentes relevantes.

Nesse sentido, é recomendável que o relatório contemple, de forma estruturada, as **principais vulnerabilidades identificadas**, ainda que não diretamente associadas a incidentes, bem como as **ações de tratamento adotadas ou planejadas**, contribuindo para o fortalecimento da transparência, para o acompanhamento da evolução dos riscos e para o aprimoramento contínuo dos controles de segurança.

4. CONCLUSÃO

A regulação relacionada a Segurança Cibernética integra um arcabouço moderno, convergente e alinhado às melhores práticas nacionais e internacionais de supervisão prudencial. Sua orientação é marcadamente **principiológica**, ao estabelecer diretrizes gerais que privilegiam a proporcionalidade, a responsabilidade institucional e a efetividade dos controles, em detrimento de prescrições excessivamente detalhadas. Nesse contexto, a norma contribui de forma estruturante para o **fortalecimento da governança corporativa**, para o **incremento da resiliência operacional** das supervisionadas e para a promoção de uma **gestão de riscos mais consistente**, favorecendo a transparência e o reforço da confiança dos agentes econômicos e da sociedade nos mercados de seguros, previdência complementar aberta, capitalização, resseguro local, cooperativismo e proteção patrimonial mutualista.