

NORMA DE SEGURANÇA DA INFORMAÇÃO NO RELACIONAMENTO COM FORNECEDORES		
Diretrizes de segurança da informação para terceiros, como fornecedores, consultores e outros.	Código do documento:	PO-CESAR-021
	Versão do documento:	2.0

ÍNDICE

1. DAS DISPOSIÇÕES PRELIMINARES	3
2. DO PROPÓSITO	3
3. DO ESCOPO	3
4. DIRETRIZES	5
5. SANÇÕES E PUNIÇÕES	5
6. REVISÕES	5
7. GESTÃO DA NORMA	6

RESPONSABILIDADE	PUBLICAÇÃO	CLASSIFICAÇÃO
ti-seguranca@cesar.org.br	22/07/2026	Pública

NORMA DE SEGURANÇA DA INFORMAÇÃO NO RELACIONAMENTO COM FORNECEDORES		
Diretrizes de segurança da informação para terceiros, como fornecedores, consultores e outros.	Código do documento:	PO-CESAR-021
	Versão do documento:	2.0

NORMA DE SEGURANÇA DA INFORMAÇÃO NO RELACIONAMENTO COM FORNECEDORES

1. DAS DISPOSIÇÕES PRELIMINARES

- 1.1. A Norma de segurança da informação no Relacionamento com Fornecedores PO-CESAR-015 complementa a Política de Segurança da Informação do CESAR, definindo as diretrizes para garantir a confidencialidade, integridade e disponibilidade das informações e a continuidade do negócio no relacionamento com os fornecedores do CESAR;
- 1.2. **Fornecedor:** Refere-se a todo e qualquer prestador de serviços, consultor, parceiro de negócios, terceiro contratado ou subcontratado, sejam pessoas físicas ou jurídicas, independentemente de contrato formal ou não, que utilizam o nome do CESAR para qualquer fim ou que prestam serviços, têm acesso aos seus dados ou ambiente, fornecem materiais, interagem com clientes ou outros em nome do CESAR para a consecução do negócio contratado.
- 1.3. **Fornecedor de risco baixo:** aquele que não irá receber/tratar dados pessoais ou dados sensíveis; que não realizará nenhum tipo de integração com sistemas internos ou ambiente do CESAR; que fornecerá serviço ou produto de uso pontual, local ou de baixo impacto em caso de falha ou incidente de segurança da informação (incluindo vazamento de dados); que terá impacto inexistente ou baixo caso ocorra alguma falha na prestação relacionada a continuidade do negócio
- 1.4. **Fornecedor de risco médio:** aquele que receberá ou tratará dados pessoais ou dados sensíveis (quer seja na situação de Operadores, no contexto da LGPD, quer sejam dados compartilhados pelo CESAR); que integrará com sistemas internos ou ambiente do CESAR; que terá impacto moderado em caso de falha ou incidente de segurança da informação (incluindo vazamento de dados); que terá impacto moderado caso ocorra alguma falha na prestação relacionada a continuidade do negócio. Para esses fornecedores, é necessária a validação do Time de Segurança da Informação e/ou TI.
- 1.5. **Fornecedor de risco alto:** aquele que tratará grande volume de dados, incluindo dados pessoais e dados sensíveis (quer seja na situação de Operadores, no contexto da LGPD, quer sejam dados compartilhados pelo CESAR); que integrará com sistemas internos ou ambiente do CESAR; que terá impacto alto ou crítico em caso de falha ou incidente de segurança da informação (incluindo vazamento de dados); que terá transferência internacional de dados envolvida na prestação de serviço; que terá impacto alto ou catastrófico caso ocorra alguma falha na prestação relacionada a continuidade do negócio; ou, ainda, fornecedores que lidem com informações de projetos com clientes ou que lidem com informações confidenciais do CESAR. Para esses, é necessário diligência completa, podendo incluir envolvimento do time jurídico, relatório de impacto a dados pessoais e outras medidas.
- 1.6. Os fornecedores passarão por análise junto ao Time de Compras do CESAR (e, em alguns casos, também ao Time de Segurança da Informação e ao Time Jurídico) para determinar sua criticidade e controles de segurança necessários de acordo com a classificação acima.

2. DO PROPÓSITO

RESPONSABILIDADE	PUBLICAÇÃO	CLASSIFICAÇÃO
ti-seguranca@cesar.org.br	22/07/2026	Pública

NORMA DE SEGURANÇA DA INFORMAÇÃO NO RELACIONAMENTO COM FORNECEDORES		
Diretrizes de segurança da informação para terceiros, como fornecedores, consultores e outros.	Código do documento:	PO-CESAR-021
	Versão do documento:	2.0

- 2.1. Estabelecer diretrizes para a segurança da informação no relacionamento com os fornecedores, incluindo o uso de equipamentos, o armazenamento de dados e documentos, e o uso de ferramentas de Inteligência Artificial no âmbito da prestação de serviços ao CESAR.

3. DO ESCOPO

- 3.1. Esta norma obedece ao escopo definido na Política de Segurança da Informação do CESAR e aplica-se a todos os equipamentos, dispositivos, sistemas e plataformas utilizados pelo fornecedor na execução dos serviços contratados, independentemente de serem de sua propriedade ou disponibilizados pelo CESAR.

4. DIRETRIZES

4.1. Uso de Equipamento

- 4.1.1. O dispositivo/notebook usado para prestar serviços/acessar remotamente dados ou o ambiente do CESAR deve ser preferencialmente de uso profissional.
- 4.1.2. Caso o fornecedor/prestador de serviços for usar o dispositivo para fins pessoais ou de entretenimento, deverá criar um perfil de acesso exclusivo para acessar dados do CESAR, seguindo as normas de senha desta norma (em especial, o item 4.3.4). É vedado o compartilhamento do perfil de usuário criado para prestar serviços ao CESAR com familiares ou quaisquer terceiros.
- 4.1.3. Para acessar, criar, editar, armazenar ou realizar qualquer outra atividade nos arquivos do CESAR, o fornecedor deverá utilizar o Google Drive oficial do CESAR, e não deve baixar os conteúdos ou manipulá-los em drives ou outros repositórios privados.
- 4.1.4. O acesso aos drives corporativos do CESAR deve ser feito exclusivamente por meio de credenciais individuais e intransferíveis, sendo vedado o compartilhamento de senhas ou credenciais de acesso entre colaboradores do fornecedor ou com terceiros não autorizados.
- 4.1.5. É vedado ao fornecedor armazenar, copiar, transferir ou manter qualquer dado, documento ou arquivo relacionado à execução dos serviços em dispositivos pessoais, unidades de armazenamento externas (pendrives, HDs externos, cartões de memória ou similares), ou serviços de armazenamento em nuvem não corporativos ou não autorizados pelo CESAR, tais como Dropbox, iCloud, OneDrive pessoal ou plataformas similares.
- 4.1.6. O CESAR não será responsável por fornecer suporte, atualização, manutenção, reposição de peças, licenciamento de softwares, reembolso ou cobrir qualquer tipo de custo referente ao uso de dispositivos pessoais ou de propriedade do cliente/fornecedor (estes 02 últimos exceto se previsto em contrato).
- 4.1.7. O uso de dispositivos de computação pessoal ou de propriedade de cliente/fornecedor para atividades de trabalho ou armazenamento de arquivos do CESAR não modifica a propriedade da organização sobre as informações criadas, armazenadas, enviadas, recebidas, modificadas ou excluídas. Permanecendo qualquer direito de propriedade intelectual com o CESAR.

RESPONSABILIDADE	PUBLICAÇÃO	CLASSIFICAÇÃO
ti-seguranca@cesar.org.br	22/07/2026	Pública

NORMA DE SEGURANÇA DA INFORMAÇÃO NO RELACIONAMENTO COM FORNECEDORES		
Diretrizes de segurança da informação para terceiros, como fornecedores, consultores e outros.	Código do documento:	PO-CESAR-021
	Versão do documento:	2.0

- 4.1.8. Ao término da prestação de serviços, por qualquer motivo, o fornecedor deverá, no prazo máximo de 5 (cinco) dias úteis contados do encerramento do vínculo contratual, confirmar por escrito ao CESAR a inexistência de cópias, reproduções ou registros de dados e documentos corporativos em dispositivos, sistemas ou plataformas não autorizados, procedendo à exclusão definitiva de eventuais arquivos armazenados em desconformidade com esta Norma.

4.2. Acesso Remoto

- 4.2.1. O acesso remoto de terceiros e prestadores de serviço a ativos/serviços de informação ou recursos computacionais do CESAR somente poderá ser concedido após a efetivação do acordo de confidencialidade entre as partes.
- 4.2.2. O acesso remoto de terceiros a ativos/serviços de informação e recursos computacionais da CESAR será concedido com os privilégios mínimos necessários para execução de suas atividades laborais.
- 4.2.3. A concessão do acesso deverá ser limitada automaticamente ao tempo necessário estimado para a atividade do terceiro ou prestador de serviço, não excedendo o máximo de seis meses por concessão; após este prazo, caso ainda seja necessário o acesso, nova concessão deverá ser solicitada através da Central de Serviços de TI por um colaborador do CESAR e com a autorização do gestor responsável pelo contrato de terceirização.
- 4.2.4. O usuário terceiro, bem como a empresa onde ele trabalha, serão os únicos responsáveis por toda ação executada com suas credenciais de acesso remoto, incluindo qualquer atividade não autorizada exercida por outras partes de posse de suas credenciais de acesso remoto.

4.3. Segurança Digital

- 4.3.1. Fornecedores que acessem ativos ou tratem dados do CESAR (incluindo informações de projetos e produtos) devem obrigatoriamente aplicar as medidas de segurança desta política em todos os equipamentos utilizados na prestação dos serviços.
- 4.3.2. É vedado utilizar o dispositivo sem qualquer proteção contra malware, vírus e outras ameaças. O fornecedor deve manter os dispositivos com alguma solução de Proteção de Endpoint (Antivírus) reconhecida, com proteção em tempo real e atualizações automáticas.
- 4.3.3. Deve-se realizar varreduras completas (*full scan*) semanalmente no equipamento utilizando o antivírus ou outra ferramenta adequada.
- 4.3.4. Senhas fortes e intransferíveis (ou biometria) devem ser implementadas para controlar o acesso ao dispositivo, incluindo a configuração de bloqueio automático de tela após, no máximo, 5 minutos de inatividade.
- 4.3.5. Os Sistemas Operacionais e navegadores devem ser mantidos devidamente licenciados e atualizados com as últimas *atualizações* de segurança, e é

RESPONSABILIDADE	PUBLICAÇÃO	CLASSIFICAÇÃO
ti-seguranca@cesar.org.br	22/07/2026	Pública

NORMA DE SEGURANÇA DA INFORMAÇÃO NO RELACIONAMENTO COM FORNECEDORES		
Diretrizes de segurança da informação para terceiros, como fornecedores, consultores e outros.	Código do documento:	PO-CESAR-021
	Versão do documento:	2.0

expressamente proibida a instalação de softwares não licenciados ou de procedência duvidosa (como aplicativos “piratas”).

- 4.3.6. Recomenda-se manter ativa a função de proteção de dados do computador, conhecida como Criptografia de Disco (Ex: BitLocker do Windows, ou FileVault do Mac), para garantir que os arquivos não sejam acessados indevidamente em eventuais casos de perda ou roubo do dispositivo.

4.4. Critérios para Fornecedores de Pequeno Porte (ME/EPP/MEI)

Fornecedores enquadrados como microempresa (ME), empresa de pequeno porte (EPP) ou microempreendedor individual (MEI) que não disponham de dispositivo exclusivo para a prestação dos serviços poderão adotar os critérios diferenciados abaixo, em substituição parcial aos requisitos da seção 4.3, desde que, cumulativamente:

- não prestem serviço classificado como crítico pelo CESAR; e
- não acessem, processem ou armazenem dados pessoais sensíveis, conforme definição da Lei nº 13.709/2018 (LGPD), no âmbito da execução do objeto contratual.

- 4.4.1. Criação e uso de uma conta de usuário do sistema operacional distinta, dedicada exclusivamente à interação com os recursos, sistemas e ambientes do CESAR, com senha forte ou autenticação biométrica, e bloqueio automático de tela após, no máximo, 5 (cinco) minutos de inatividade.
- 4.4.2. Armazenamento de dados do CESAR restrito exclusivamente aos drives corporativos por ele designados.
- 4.4.3. Manutenção do sistema operacional e de todos os aplicativos instalados atualizados, com aplicação das atualizações de segurança em dia.
- 4.4.4. Vedação à instalação de softwares de procedência desconhecida ou "pirata", obtidos fora das lojas oficiais dos fabricantes ou de repositórios reconhecidos.
- 4.4.5. Utilização de alguma ferramenta antivírus, nativa ou de terceiros, mesmo que gratuita, desde que reconhecida pelo mercado (ex.: Malwarebytes Free, Kaspersky Security Cloud Free ou equivalente).

4.5. Proteção de dados pessoais

- 4.5.1. O fornecedor deve conhecer e obedecer a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD).
- 4.5.2. O fornecedor compromete-se a tratar os dados pessoais exclusivamente para as finalidades definidas pelo CESAR e de acordo com as instruções formais recebidas.
- 4.5.3. O fornecedor deverá seguir as orientações do CESAR quanto ao uso, armazenamento e compartilhamento de dados pessoais, respeitando os princípios e obrigações previstos na LGPD.
- 4.5.4. O fornecedor deverá cooperar com o CESAR no atendimento a solicitações de titulares de dados, autoridades competentes e na elaboração de relatórios de

RESPONSABILIDADE	PUBLICAÇÃO	CLASSIFICAÇÃO
ti-seguranca@cesar.org.br	22/07/2026	Pública

NORMA DE SEGURANÇA DA INFORMAÇÃO NO RELACIONAMENTO COM FORNECEDORES		
Diretrizes de segurança da informação para terceiros, como fornecedores, consultores e outros.	Código do documento:	PO-CESAR-021
	Versão do documento:	2.0

impacto à proteção de dados pessoais, dentro da legalidade e razoabilidade e no escopo em que lhe couber.

- 4.5.5. A contratação de sub-operadores pelo fornecedor exige autorização prévia do CESAR. O fornecedor garante que seus sub-operadores estarão vinculados às mesmas obrigações de proteção de dados e segurança previstas nesta política.
- 4.5.6. Ao término da prestação do serviço, o fornecedor compromete-se a eliminar de forma definitiva ou devolver ao CESAR todos os dados pessoais tratados, incluindo cópias e backups, salvo se houver obrigação legal expressa para a retenção

4.6. Uso de Ferramentas de Inteligência Artificial

Esta seção observa as diretrizes gerais de governança de Inteligência Artificial do CESAR. Em caso de divergência quanto a ferramentas ou usos específicos, prevalece a orientação da área de Segurança da Informação.

- 4.6.1. É expressamente vedada a inserção, em quaisquer plataformas, ferramentas ou sistemas de Inteligência Artificial, de dados confidenciais, estratégicos, pessoais ou sensíveis pertencentes ao CESAR, a seus clientes, parceiros ou projetos, incluindo, sem limitação: conteúdos internos de qualquer natureza; documentos, estudos, relatórios e materiais de pesquisa e desenvolvimento (P&D); informações de clientes, parceiros ou fornecedores do CESAR; e quaisquer outros materiais que possam comprometer a confidencialidade, a segurança ou a propriedade intelectual do CESAR.
- 4.6.2. Qualquer utilização de ferramentas de IA que vá além do uso genérico e não relacionado ao objeto contratual dependerá de aprovação prévia e expressa da área de Segurança da Informação do CESAR, que poderá estabelecer condições específicas, impor restrições ou vedar determinados usos, conforme critérios técnicos e de conformidade que entender pertinentes.
- 4.6.3. O fornecedor deverá orientar e conscientizar seus colaboradores, prepostos e subcontratados eventualmente autorizados acerca das restrições previstas nesta cláusula, sendo responsável por qualquer violação decorrente do uso indevido de ferramentas de IA por pessoas a ele vinculadas.
- 4.6.4. O CESAR poderá, a qualquer tempo, atualizar a lista de ferramentas de IA autorizadas ou restritas, comunicando o fornecedor por escrito, sendo que as novas restrições passarão a vigorar imediatamente após a comunicação.
- 4.6.5. O uso de ferramentas de IA em conformidade com esta cláusula não exime o fornecedor de suas demais obrigações de confidencialidade, proteção de dados e segurança da informação previstas nesta Norma.

4.7. Comunicação de Incidentes

RESPONSABILIDADE	PUBLICAÇÃO	CLASSIFICAÇÃO
ti-seguranca@cesar.org.br	22/07/2026	Pública

NORMA DE SEGURANÇA DA INFORMAÇÃO NO RELACIONAMENTO COM FORNECEDORES		
Diretrizes de segurança da informação para terceiros, como fornecedores, consultores e outros.	Código do documento:	PO-CESAR-021
	Versão do documento:	2.0

- 4.7.1. A comunicação de qualquer suspeita ou confirmação de incidente de segurança da informação/proteção de dados pessoais é crítica para a segurança do CESAR. Qualquer alerta de malware persistente, perda de dispositivo ou incidente que impacte informações corporativas deve ser comunicado à equipe de TI/Segurança do CESAR em um prazo não superior a 24 (vinte e quatro) horas.
- 4.7.2. Em casos de acesso não autorizado, extravio, furto ou roubo de dispositivos computacionais que tenham o acesso remoto ao ambiente do CESAR habilitado, o usuário responsável deverá informar imediatamente o ocorrido à equipe de segurança da informação do CESAR por meio do registro de um incidente de segurança da informação.
- 4.7.3. Caso se aplique, o fornecedor deve possuir canais claros para que seus funcionários reportem incidentes internamente e os escalem imediatamente ao CESAR.

4.8. Conformidade e Acesso à Informação

- 4.8.1. Caso se aplique, o fornecedor deve manter acordos de confidencialidade e termos de responsabilidade assinados por todos os seus colaboradores, prevendo medidas disciplinares em caso de descumprimento.
- 4.8.2. O fornecedor deve permitir a realização de visitas ou avaliações periódicas por parte do CESAR para verificação de controles. A frequência será determinada pela criticidade do negócio.
- 4.8.3. Quando solicitado, o fornecedor deve preencher o Checklist de Segurança para fornecedores do CESAR, que poderá ser apresentado antes da contratação e também depois, em ciclos de revisão e acompanhamento da situação do fornecedor.
- 4.8.4. O CESAR poderá realizar auditorias ou inspeções a qualquer tempo durante a vigência do contrato, destinadas a verificar o cumprimento das disposições desta Norma, mediante comunicação prévia por escrito com antecedência mínima razoável, salvo em casos de suspeita de incidente de segurança, nos quais a auditoria poderá ser realizada imediatamente. O fornecedor deve, ainda, manter registro atualizado dos equipamentos utilizados na execução dos serviços, disponibilizando-o ao CESAR sempre que solicitado, para fins de auditoria e verificação de conformidade.
- 4.8.5. O fornecedor deverá cooperar plenamente com as auditorias realizadas pelo CESAR, fornecendo acesso às informações, documentos, sistemas e evidências necessários à verificação de conformidade, no prazo e nas condições indicados pelo CESAR.
- 4.8.6. O CESAR poderá, igualmente, contratar terceiros especializados para a realização das auditorias previstas nesta cláusula, sendo que os auditores externos estarão sujeitos às mesmas obrigações de confidencialidade aplicáveis às partes.
- 4.8.7. Os resultados das auditorias realizadas serão compartilhados com o fornecedor, que deverá, no prazo estabelecido pelo CESAR, apresentar plano de ação para correção de eventuais não conformidades identificadas.

RESPONSABILIDADE	PUBLICAÇÃO	CLASSIFICAÇÃO
ti-seguranca@cesar.org.br	22/07/2026	Pública

NORMA DE SEGURANÇA DA INFORMAÇÃO NO RELACIONAMENTO COM FORNECEDORES		
Diretrizes de segurança da informação para terceiros, como fornecedores, consultores e outros.	Código do documento:	PO-CESAR-021
	Versão do documento:	2.0

- 4.8.8. A realização de auditorias pelo CESAR não implica a assunção de qualquer responsabilidade por parte deste em relação às práticas de segurança da informação adotadas pelo fornecedor, permanecendo este integralmente responsável pelo cumprimento das obrigações previstas nesta Norma.
- 4.8.9. Identificado o descumprimento de qualquer requisito de segurança previsto nesta Norma, o CESAR poderá determinar a imediata suspensão do acesso do fornecedor a seus sistemas, ambientes e informações, até que a conformidade seja restabelecida, sem que tal medida configure inadimplemento contratual por parte do CESAR.
- 4.8.10. O fornecedor deverá adotar, ainda, todas as demais medidas técnicas e organizacionais razoavelmente necessárias para garantir a segurança dos equipamentos, dados e ambientes utilizados na execução dos serviços, mesmo que não expressamente previstas nesta Norma, sempre que tais medidas forem recomendadas pelas melhores práticas de segurança da informação vigentes.

5. SANÇÕES E PUNIÇÕES

- 5.1. O não cumprimento das disposições de segurança digital e das obrigações de reporte de incidentes sujeitará o fornecedor às penalidades previstas em contrato, as quais serão analisadas pelo departamento Jurídico conforme a gravidade da violação.

6. DISPOSIÇÕES FINAIS

- 6.1. Esta norma não substitui cláusulas contratuais específicas, podendo ser complementada por requisitos adicionais previstos em contrato, acordos de nível de serviço (SLA) ou termos específicos de segurança.
- 6.2. Em caso de conflito entre as disposições desta Norma e as de um contrato específico firmado com um fornecedor, prevalecerão as disposições que ofereçam maior proteção à segurança da informação e aos dados do CESAR.
- 6.3. A tolerância do CESAR em relação ao eventual descumprimento de qualquer disposição desta Norma não poderá ser interpretada como renúncia ao direito de exigir o seu cumprimento integral no futuro, nem como novação das obrigações aqui estabelecidas.
- 6.4. Caso qualquer disposição desta Norma seja considerada nula, inválida ou inexecutável, as demais disposições permanecerão em pleno vigor e efeito, devendo o CESAR e o fornecedor buscar, de boa-fé, a substituição da disposição afetada por outra que produza efeitos equivalentes e esteja em conformidade com a legislação aplicável.
- 6.5. Quaisquer dúvidas, omissões ou situações não previstas nesta Norma deverão ser submetidas à área de Segurança da Informação do CESAR (ti-seguranca@cesar.org.br), cuja orientação prevalecerá para fins de interpretação e aplicação das regras aqui estabelecidas.
- 6.6. As obrigações previstas nesta Norma que, por sua natureza, devam perdurar além do término da relação com o fornecedor — especialmente aquelas relacionadas à confidencialidade, à proteção de dados e à exclusão de informações — permanecerão vigentes pelo prazo estabelecido no contrato principal ou, na ausência de previsão específica, pelo prazo de 2 (dois) anos contados do encerramento do vínculo contratual.

RESPONSABILIDADE	PUBLICAÇÃO	CLASSIFICAÇÃO
ti-seguranca@cesar.org.br	22/07/2026	Pública

NORMA DE SEGURANÇA DA INFORMAÇÃO NO RELACIONAMENTO COM FORNECEDORES		
Diretrizes de segurança da informação para terceiros, como fornecedores, consultores e outros.	Código do documento:	PO-CESAR-021
	Versão do documento:	2.0

7. REVISÕES

- 7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do COMITÊ DE SEGURANÇA DA INFORMAÇÃO.

8. GESTÃO DA NORMA

- 8.1. A norma de relacionamento com fornecedores é aprovada pelo COMITÊ DE SEGURANÇA DA INFORMAÇÃO em conjunto com a Diretoria do CESAR.

RESPONSABILIDADE	PUBLICAÇÃO	CLASSIFICAÇÃO
ti-seguranca@cesar.org.br	22/07/2026	Pública