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:	1.0

ÍNDICE

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

2.1. Estabelecer diretrizes para a segurança da informação no relacionamento com os fornecedores.

3. DO ESCOPO

3.1. Esta norma obedece ao escopo definido na Política de Segurança da Informação do 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 de uso estritamente profissional. É vedado o uso para fins pessoais ou de entretenimento (jogos, redes sociais, streamings), visando manter a integridade e a segurança do dispositivo ao trafegar pela internet e baixar conteúdo.

4.1.2. 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.

4.1.3. É vedado o compartilhamento de dispositivos ou perfis de usuário com familiares ou terceiros. O acesso ao equipamento é restrito ao fornecedor e à sua equipe profissional, desde que formalmente autorizada para a execução dos serviços ao CESAR.

4.1.4. 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).

4.1.5. 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.

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.

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

4.3.6. Deve ser mantida 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. Proteção de dados pessoais

4.4.1. O fornecedor deve conhecer e obedecer a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD).

4.4.2. O fornecedor compromete-se a tratar os dados pessoais exclusivamente para as finalidades definidas pelo CESAR e de acordo com as instruções formais recebidas.

4.4.3. 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.

4.4.4. O fornecedor deverá cooperar com o CESAR no atendimento a solicitações de titulares de dados, autoridades competentes e na elaboração de relatórios de

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

4.4.5. 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.

4.4.6. 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

4.5. Comunicação de Incidentes

4.5.1. 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.

4.5.2. 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.

4.5.3. Caso se aplique, o fornecedor deve possuir canais claros para que seus funcionários reportem incidentes internamente e os escalem imediatamente ao CESAR.

4.6. Conformidade e Acesso à Informação

4.6.1. 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.

4.6.2. 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.

4.6.3. 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.

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.

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.