Diretrizes de CiberSegurança

RD Saúde

APLICABILIDADE: As disposições desta diretriz aplicar-se-ão exclusivamente às hipóteses em que a execução do Contrato envolva Itens de Cibersegurança. Na ausência de Itens de Cibersegurança, as referidas disposições não produzirão efeitos entre as Partes.

1. DEFINIÇÕES

Contratada: toda pessoa física ou jurídica que, a qualquer título, mantenha relacionamento comercial ou contratual com a RD Saúde para o fornecimento de bens, prestação de serviços, execução de obras, desenvolvimento de soluções, disponibilização de tecnologias ou realização de qualquer atividade em seu interesse ou benefício, independentemente da natureza, forma ou duração da contratação. Consideram-se igualmente abrangidos os seus sócios, administradores, diretores, empregados, colaboradores, estagiários, representantes, procuradores, consultores, prepostos, subcontratados, afiliadas, terceiros por ela contratados e quaisquer pessoas que atuem sob sua responsabilidade ou em seu nome no desempenho das atividades relacionadas ao objeto da contratação, na medida de sua atuação.

Incidente de Segurança: qualquer evento, confirmado ou suspeito, que envolva violação de políticas de segurança, acesso não autorizado, indisponibilidade de sistemas, malware, ataques cibernéticos ou qualquer outra situação que represente risco aos ativos ou continuidade de negócios da **RD Saúde**.

Itens de Cibersegurança: qualquer um dos seguintes escopos: (i) acesso ou integração a sistemas, redes, ambientes em nuvem ou infraestrutura da **RD Saúde**; (ii) oferta de solução de software (SaaS ou on-premise) que se conecte ao ambiente da **RD Saúde**; (iii) acesso remoto ao ambiente da **RD Saúde**; (iv) hospedagem de dados em nome da **RD Saúde**; (v) acesso a código-fonte, repositórios ou autorização para commit de novos códigos; (vii) suporte a operações críticas de negócio cuja falha possa impactar a operação.

2. DISPOSIÇÕES APLICÁVEIS

Gestão de Ativos e Controle de Acesso

A **Contratada** deverá manter inventário atualizado dos ativos de informação utilizados na execução dos serviços contratados, incluindo hardware, software, dados e recursos humanos. Também deverá realizar avaliações periódicas de riscos relacionados à segurança da informação, documentando vulnerabilidades, ameaças e impactos potenciais, com base em metodologias reconhecidas.

A **Contratada** deverá garantir que o acesso aos sistemas, redes, infraestrutura ou ambientes em nuvem da **RD Saúde** seja realizado exclusivamente por usuários autorizados pela **RD Saúde**, mediante autenticação forte (ex.: autenticação multifator), com perfis de acesso compatíveis com suas funções e responsabilidades.

É vedado o compartilhamento de credenciais de acesso entre usuários. A **Contratada** deverá manter controle e registro de todas as credenciais utilizadas, bem como garantir sua proteção contra vazamentos, uso indevido ou acesso não autorizado.

Registros, Auditoria e Monitoramento

A **Contratada** deverá manter, por no mínimo 12 (doze) meses, registros de acesso e atividades realizadas nos sistemas, redes ou infraestrutura da **RD Saúde**, e disponibilizá-los à **RD Saúde** em até 5 (cinco) dias a contar da data de solicitação, sempre que solicitado. A **RD Saúde** poderá realizar auditorias periódicas para verificar o cumprimento das obrigações de segurança.

Gestão e Comunicação de Incidentes de Segurança

A **Contratada** compromete-se a implementar e manter durante toda a vigência deste Contrato um processo formal de gestão de Incidentes de Segurança, com capacidade de detecção, análise, contenção, erradicação, recuperação e comunicação de eventos que possam comprometer a confidencialidade, integridade ou disponibilidade dos ativos da **Contratada**.

A **Contratada** deverá comunicar à **RD Saúde** qualquer Incidente de Segurança que envolva, direta ou indiretamente, os ativos da **RD Saúde**, no prazo máximo de 24h (vinte e quatro horas após sua detecção, por meio dos canais previamente acordados. A comunicação deverá conter, no mínimo: (i) data e hora da detecção; (ii) descrição preliminar do Incidente de Segurança; (iii) sistemas, dados ou serviços afetados; e (iv) medidas iniciais adotadas pela(s) **Contratada**.

Sempre que houver um Incidente de Segurança a **Contratada** deverá:

(a) conduzir investigação detalhada do Incidente de Segurança e apresentar à **RD Saúde**, em até 5 (cinco) dias úteis contados da data de sua detecção, um relatório técnico contendo: (i) causa raiz do Incidente de Segurança; (ii) impacto estimado; (iii) evidências coletadas; (iv) medidas corretivas e preventivas adotadas pela **Contratada**; e (v) plano de ação para evitar recorrência; e

(b) cooperar integralmente com a **RD Saúde** e, quando aplicável, com autoridades reguladoras ou legais, fornecendo acesso às informações, registros e evidências necessárias para apuração dos fatos e mitigação dos impactos.

Continuidade de Negócios e Recuperação de Desastres

A **Contratada** deverá possuir plano de continuidade de negócios e recuperação de desastres que contemple cenários de Incidentes de Segurança, garantindo a retomada dos serviços em tempo hábil e com mínima perda de dados.

Todos os registros relacionados à gestão de Incidentes de Segurança deverão ser mantidos pela **Contratada** por um período mínimo de 24 (vinte e quatro) meses, e disponibilizados à **RD Saúde** sempre que solicitado.

Ambientes em Nuvem e Segurança da Informação

Caso os serviços envolvam ambientes em nuvem, a **Contratada** deverá garantir que os provedores utilizados estejam em conformidade com normas internacionais de segurança da informação (ex.: ISO/IEC 27001, SOC 2), e que os dados da **RD Saúde** estejam segregados logicamente de outros clientes.

Capacitação e Conscientização

A **Contratada** deverá assegurar que seus colaboradores envolvidos na execução do contrato recebam treinamentos periódicos sobre segurança da informação e boas práticas de uso dos sistemas da **RD Saúde**.

Avaliação de Riscos Cibernéticos de Terceiros

A **Contratada** compromete-se a submeter-se e colaborar com a avaliação de riscos cibernéticos de terceiros conduzida pela **RD Saúde**, conforme metodologia, critérios e periodicidade definidos por esta. Essa avaliação poderá incluir, entre outros, o preenchimento de questionários, entrevistas, auditorias, análise documental e verificação de controles técnicos e organizacionais relacionados à segurança da informação.

A **RD Saúde** reserva-se o direito de reavaliar a **Contratada** sempre que houver alterações significativas nos serviços prestados, Incidentes de Segurança, ou mudanças no ambiente regulatório