ANEXO VIII – ESPECIFICIDADES DO SISTEMA WEB

O sistema web da contratada deverá apresentar as seguintes característica de segurança e funcionalidades:

1 – O sistema web deve apresentar disponibilidade mínima de 99,5% (noventa e nove inteiros e 5 décimos por cento). O fornecedor deverá informar o ambiente de hospedagem da solução, incluíndo país, região e datacenter ou provedor de nuvem, garantindo SLA mínimo de 99,5 % de disponibilidade mensal, com mecanismos de redundância e planos de contingência. Deverá ser apresentada política formal de backup periódico e automático, com retenção mínima de 90 (noventa) dias, procedimentos de restauração sob demanda com prazos definidos, e armazenamento seguro e criptografado dos dados. O MPRS poderá solicitar, a qualquer momento, o acesso aos backups armazenados.

2 – O Sítio de hospedagem do sistema web deve possuir certificação SECURE SOCKETS LAYER.

3 – A aplicação deve ser resistente aos principais vetores de ataque WEB listados no OWASP top 10.

4 – Acesso ao log de dados e de auditoria do sistema web:

O sistema deve manter logs de auditoria imutáveis, registrando no mínimo: IP de origem e a porta lógica da conexão, data e hora (timestamp exato, preferencialmente em milissegundos no padrão UTC). Esses logs devem ser acessíveis para auditoria e controle interno, sempre que solicitados pelo MPRS, com período de retenção mínimo de noventa dias, garantindo a rastreabilidade e unicidade da origem em caso de incidentes.

5 – Em relação aos itens 4, 5, 6 e 7 da Prova de Conceito, Anexo VII, o sistema web deve ter integração ao Active Directory (AD), na modalidade Azure AD, com MFA obrigatório.

O sistema deve ter capacidade nativa de integração com serviços de diretório Azure AD (Azure Active Directory):

O sistema deve suportar autenticação federada com Azure AD usando protocolos como OAuth 2.0, OpenID Connect ou SAML 2.0. Deve ser compatível com Multi-Factor Authentication (MFA), conforme as políticas do Azure AD, e com Azure AD B2B para acesso controlado de usuários externos convidados. Deve ser possível configurar múltiplos domínios e Unidades Organizacionais (OUs), além de mapear grupos específicos do AD para perfis de acesso no sistema. A sincronização de usuários poderá ser automática ou sob demanda.

O sistema deverá suportar autenticação multifator (MFA) para todos os usuários, em conformidade com as políticas de segurança da instituição. A solução deverá ser compatível com os mecanismos de MFA já adotados pelo órgão, incluindo, preferencialmente, o Microsoft Authenticator, ou outros baseados em padrões amplamente utilizados no mercado.

O sistema deverá implementar mecanismo de controle de acesso baseado em papéis (RBAC), permitindo a definição de perfis de acesso conforme funções institucionais. Cada papel deverá possuir permissões

específicas e configuráveis, com possibilidade de associação automática a partir de grupos ou unidades organizacionais do Azure AD.

6 – A comunicação entre browser e servidor deve ser criptografada:

A comunicação entre o browser/cliente e o servidor deve ser criptografada, utilizando protocolos seguros como TLS (Transport Layer Security) versão 1.2 ou superior, forçando a utilização do mecanismo HSTS

(HTTP Strict Transport Security), para garantir a confidencialidade e integridade dos dados trafegados, independentemente da arquitetura de implementação (on-premise ou nuvem).

7 – O sistema deverá estar em plena conformidade com a Lei Geral de Proteção de Dados (LGPD), apresentando política de privacidade atualizada, identificação do Encarregado de Dados (DPO) e mecanismos para garantir o exercício dos direitos dos titulares (acesso, retificação, exclusão e portabilidade de dados).

Em caso de incidente de segurança envolvendo vazamento de dados ou violação de credenciais de acesso, o fornecedor deverá comunicar formalmente o MPRS no prazo máximo de 72 (setenta e duas) horas a partir da identificação do ocorrido.