Questionário de Segurança da Informação

O presente documento visa responder a questões sobre os métodos e procedimentos adotados pela CentralServer para permitir o acesso a recursos computacionais e dados por parte de colaboradores e clientes, devidamente identificados e autorizados, segundo padrões internacionais de gestão da segurança da informação e em consonância com a legislação vigente.

INTRODUÇÃO	
Quais os tipos de serviços oferecidos?	IaaS, CloudOps, Email.
Quais os ambientes de computação em nuvem suportados?	VMware Cloud, Amazon Web Services (AWS) e Microsoft Azure.
Detalhamento:	**IaaS:** infraestrutura de computação em nuvem fornecida como serviço para consumo sob demanda ou pré-alocado. **CloudOps:** operação de IaaS ou de Ambiente Operacional dentro de escopo especificado e segundo rotinas pré-definidas. **Email:** serviço de correio eletrônico com infraestrutura dedicada para o cliente. **VMware:** serviço de data center virtual da CentralServer baseado em infraestrutura Equinix, tecnologia VMware e painéis de autosserviço para provisionamento, controle e monitoramento de recursos. **AWS:** serviço de nuvem pública da Amazon Web Services. **Azure:** serviço de nuvem pública da Microsoft Azure.

INFRAESTRUTURA VMWARE CLOUD		
1	Qual a classificação de disponibilidade do data center?	Estrutura Equinix certificada padrão Tier III, zonas de proteção contra incêndios, sistemas redundantes de energia (2N) e ar condicionado (N+20%).
2	Quais as normas e certificações do data center?	A Equinix segue padrões de referência para a estrutura de data center, conforme informado em: https://www.equinix.com.br/services/data-centers-colocation/standards-compliance/ A VMware possui certificações de segurança apresentadas em: https://www.vmware.com/security/certifications.html

		A CentralServer é parceira certificada VMware, conforme informado em: https://www.centralserver.com/br/sobre-nos/
3	Em qual localidade está localizado o data center?	Tamboré - São Paulo (Equinix).
4	A infraestrutura possui redundância para alta disponibilidade?	A energia que alimenta os equipamentos é 100% redundante fazendo o uso de fontes e circuitos elétricos duais, nobreaks e grupos motor-gerador. As conexões de rede são redundantes com base em diferentes operadoras de telecomunicações. Os roteadores de borda, core e topo de rack, assim como os sistemas de firewall, são redundantes. Os servidores operam em cluster de alta disponibilidade com tecnologia VMware.
5	A infraestrutura possui escalabilidade horizontal e vertical?	Sim, com base na tecnologia de virtualização.
6	A infraestrutura faz uso de balanceadores de carga para distribuição em múltiplos servidores?	Funcionalidade disponível (opcional).

INFRAESTRUTURA AWS		
7	Quais as normas e certificações do data center?	A AWS segue padrões de referência para a estrutura de seus data centers, conforme informado em: https://aws.amazon.com/compliance/data-center/data-centers/ https://aws.amazon.com/compliance/uptimeinstitute/
8	Quais as normas e certificações obtidas?	A AWS possui certificações de referência, conforme informado em: https://aws.amazon.com/compliance/programs/ A CentralServer é parceira certificada AWS, conforme informado em: https://www.centralserver.com/br/sobre-nos/

INFRAESTRUTURA AZURE		
9	Quais as normas e certificações do data center?	A Azure segue padrões de referência para a estrutura de seus data centers, conforme informado em: https://azure.microsoft.com/pt-br/global-infrastructure/ https://azure.microsoft.com/pt-br/overview/trusted-cloud/
10	Quais as normas e certificações obtidas?	A Azure possui certificações de referência, conforme informado em: https://azure.microsoft.com/pt-br/overview/trusted-cloud/compliance/ A CentralServer é parceira certificada Microsoft e Azure, conforme informado em: https://www.centralserver.com/br/sobre-nos/

CONTINUIDADE DE NEGÓCIOS		
11	Qual o processo de backup de dados e os tempos em que são realizados?	Mecanismo de geração backups “full” e incrementais das máquinas virtuais (opcional). Backup off-site disponível (opcional).
12	Os backups estão criptografados?	Criptografia de dados armazenados disponível (opcional).
13	Por quanto tempo os backups são armazenados?	Período de retenção de dados de backup disponível em dias, meses ou anos (opcional).
14	Quais as formas de backup disponíveis?	VMware: backup realizado via ferramenta Veeam em storages separados dos clusters de produção (opcional). AWS e Azure: backup realizado via snapshots de volumes de disco em object storage (opcional).
15	Qual o mecanismo disponível para recuperação de desastres?	Uso das nuvens AWS e Azure para implantação de plano de recuperação de desastres e continuidade de negócios (opcional).
16	Qual o tempo necessário para a recuperação dos serviços em caso de desastre?	15 a 240 minutos, conforme o projeto (opcional).
17	Qual a periodicidade de realização de testes de recuperação de desastres?	Trimestral ou semestral (opcional).

MONITORAMENTO DE RECURSOS		
18	Como são monitorados os recursos do data center?	VMware: sistemas de monitoramento internos e externos ao data center que permitem monitorar a carga, a disponibilidade e o desempenho dos recursos computacionais, além de configurar endereços de email e telefones para recebimento de alertas. A CentralServer monitora os servidores, roteadores, firewalls e o tráfego da rede em regime 24x7. AWS e Azure: o monitoramento da infraestrutura é realizado pelos respectivos fornecedores em regime 24x7.
19	Como são monitoradas as máquinas virtuais, servidores web, bancos de dados e demais aplicações?	VMware: através de sistema de monitoramento que faz uso de programas “agentes” instalados a nível de sistema operacional. AWS e Azure: através das ferramentas de monitoramento nativas das nuvens e, opcionalmente, via “agentes” instalados a nível de sistema operacional. Em todos os ambientes, a CentralServer e o cliente têm diferentes níveis de visibilidade e responsabilidade de atuação dependendo do escopo de gerenciamento contratado (opcional).

SEGURANÇA FÍSICA		
20	Como funciona a segurança física do data center?	VMware: acesso às instalações prediais, salas e racks restrito a pessoal previamente cadastrado e autorizado, mediante apresentação de identificação pessoal. Deslocamentos internos controlados via crachá e biometria. Lista de pessoas autorizadas é revisada sempre que ocorre mudança de pessoal. Sistema de eclusa na portaria, porta controlada na recepção e detector de metais. Hardware entrante é controlado e identificado para efeito de rastreamento. Sistema de monitoramento por câmeras nas salas, corredores e gaiolas de racks. Portas de acesso integradas à rede de no-break, com comutação para estado de travamento no caso de falta de energia. AWS e Azure: controle de acesso realizado pelos respectivos fornecedores.
21	Qual o sistema de proteção contra incêndio utilizado no data center?	VMware: sistema de proteção contra incêndios com gás FM-200. AWS e Azure: proteção de incêndio implantada pelos respectivos fornecedores.
22	Qual o procedimento de descarte de discos rígidos em casos de manutenção?	VMware: recolhimento para laboratório, desmontagem, inutilização e descarte para reciclagem. AWS e Azure: procedimento executado pelos respectivos fornecedores.

SEGURANÇA LÓGICA		
23	O acesso à rede do data center é protegido por firewalls?	Firewalls multicamada redundantes com funções stateless e stateful usados para proteção da rede.
24	Como são protegidos os acessos remotos aos sistemas da infraestrutura?	VMware: operadores da CentralServer acessam os sistemas via link dedicado ou rede privada virtual (VPN). Clientes têm a possibilidade de acessar seus recursos via link dedicado (opcional), VPN (opcional), protocolo SSL e também usar “vlans” para segmentar de rede e formar DMZs (opcional).

		AWS e Azure: operadores da CentralServer usam as credenciais da empresa na nuvem pública para acessar os recursos cujo acesso foi delegado na conta do cliente. Clientes usam os mecanismos de acesso e autenticação fornecidos pela nuvem pública.
25	Como é feita a proteção da rede contra ataques?	VMware: rede protegida por access-lists em roteadores e regras de firewall. VLANS para isolamento de redes lógicas e de máquinas virtuais (opcional). Mecanismo anti-DDoS para proteção da rede do data center. AWS e Azure: sistemas de proteção da rede controlados pelos respectivos fornecedores.
26	Há sistemas para proteção contra vírus e intrusos?	Disponibilidade de sistemas antivírus e anti-intrusão disponíveis a nível de infraestrutura e sistema operacional (opcional).
27	Como é feito o isolamento de recursos entre os clientes do data center?	VMware: segmentações físicas e lógicas de rede (vlans). Controle de ARP para proteção anti-spoofing. Microsegmentação para isolamento de máquinas virtuais (opcional). AWS e Azure: isolamento de recursos implantado por mecanismos específicos de cada fornecedor.

	OPERAÇÕES	
28	Como são tratadas as solicitações de serviços?	Abertura de chamados via Portal de Relacionamento, console de autosserviço ou aplicativo de mensagem por usuários previamente cadastrados no console de autosserviço.
29	Os procedimentos operacionais são documentados e controlados?	Procedimentos operacionais documentados, revisados regularmente e organizados em base de conhecimento acessível pela equipe interna.
30	Há segregação de funções na equipe para restringir o acesso aos ativos de tecnologia da informação?	Colaboradores com nível de acesso diferenciado para acesso a sistemas e dados de clientes.
31	Como são realizados os procedimentos de manutenção?	Manutenções realizadas via processo de Gestão de Mudança (GMUD) com avaliação de risco e impacto, abertura de janela de manutenção, comunicados aos stakeholders e procedimento de reversão definido.
32	Quais os procedimentos de gestão de incidentes?	A remediação de incidentes pode ser realizada automaticamente pelo sistema de monitoramento ou pelas equipes de Suporte Técnico e de Operações da CentralServer, de acordo com nível de severidade e escopo contratado pelo cliente. Incidentes relacionados a vulnerabilidades, falhas de segurança ou uso abusivo resultam na remoção ou isolamento do recursos afetados para posterior investigação da causa raiz e tomada de ações corretivas. Ataques de DoS ou DDoS resultam no bloqueio da origem, filtragem de pacotes ou isolamento do destino do tráfego para proteção da rede do data

		center. O cliente é informado a respeito do incidente e das ações tomadas por meio de notificações e pareceres técnicos.
33	Existe a separação dos recursos de desenvolvimento, teste e produção?	Ambientes de desenvolvimento, teste e produção dos sistemas devidamente implantados.
34	Como funciona o controle de versões de software e a aplicação de correções de segurança?	VMware: uso de repositórios Git para versionamento do console de autosserviço e sistemas de gestão. Controle de versão e aplicação de atualizações da infraestrutura VMware via Update Manager. Softwares de controle de versão e aplicação de atualizações disponíveis para sistemas operacionais Windows (WSUS, Plesk) e Linux (Spacewalk, Plesk, KernelCare), com aplicação das atualizações automaticamente ou via processo de GMUD. AWS e Azure: controle de versão e aplicação de atualizações da infraestrutura via mecanismos específicos de cada fornecedor. Softwares de controle de versão e aplicação de atualizações disponíveis para sistemas operacionais Windows (WSUS, Plesk) e Linux (Spacewalk, Plesk, KernelCare), com aplicação das atualizações automaticamente ou via processo de GMUD.

GOVERNANÇA DE DADOS		
35	Existe uma política de segurança da informação aplicada aos funcionários e terceiros?	Política de Segurança da Informação existente e apresentada aos colaboradores internos e a prestadores de serviço quando aplicável.
36	Os colaboradores da empresa assinam um documento formal com cláusulas de privacidade e confidencialidade dos dados e informações?	Acordo de privacidade e confidencialidade assinado por todos os colaboradores e fornecedores que têm acesso a dados e sistemas da empresa.
37	Existe um processo de análise de riscos e formas definidas de mitigação de problemas de segurança?	Comitê interno para análise de riscos e impactos sobre segurança e privacidade com reuniões quinzenais ou em caráter extraordinário quando necessário.
38	A equipe recebe treinamentos periódicos de boas práticas de segurança da informação?	Treinamentos de novos colaboradores e reuniões regulares com a equipe para apresentação de normas e orientações sobre boas práticas de segurança da informação.
39	As credenciais são individuais para garantir que os acessos sejam identificados?	Uso de credenciais individuais para colaboradores internos, operadores de data center e usuários do console de autosserviço, exceto em sistemas que não permitam a individuação de logins administrativos.
40	Onde ficam armazenadas as credenciais individuais?	Em controladores de domínio e registros criptografados em bases de dados de sistemas. Colaboradores internos, incluindo operadores do data center, usam cofre de senhas para armazenamento das credenciais.

41	Qual a política de senha adotada?	Senhas com tamanho mínimo de 12 caracteres no console de autosserviço. Colaboradores internos, incluindo operadores de data center, usam senhas com, no mínimo, 16 caracteres renovadas periodicamente.
42	O acesso ao console de autosserviço é protegido por diferentes perfis de acesso e autenticação multifator?	Login no console de autosserviço com suporte a autenticação de dois fatores (2FA) e níveis diferenciados de acesso: gestor da conta, técnico total, leitor total, técnico leitura e leitor faturas.
43	Como é feito o registro e a auditoria de acessos ao ambiente?	Acessos e operações feitos no console de autosserviço são registrados no log da aplicação e disponibilizados para consulta pelos operadores do data center. Os clientes podem consultar os acessos e operações feitos pelos usuários da sua entidade. Os acessos aos recursos gerenciados pela CentralServer são registrados em logs de serviço quando esse tipo de facilidade é disponibilizada pelo fabricante.

TERMOS DE USO E POLÍTICA DE PRIVACIDADE		
44	A empresa tem definidos os termos de uso dos serviços?	Termos de Uso definidos e disponíveis para consulta em: https://www.centralserver.com/br/termos-de-uso/
45	A empresa tem definida uma política de privacidade e tratamento de dados pessoais?	Política de Privacidade implementada e disponível para consulta em: https://www.centralserver.com/br/politica-de-privacidade/

AVISO LEGAL: O presente documento tem por objetivo descrever o ambiente e as práticas de gestão da segurança da informação adotadas pela CentralServer. A CentralServer se reserva o direito de modificar a qualquer tempo e sem aviso prévio as informações aqui apresentadas a fim de refletir o lançamento de novos serviços, as atualizações físicas e operacionais, e a evolução do estado-da-arte da tecnologia. Quando ocorrer a alteração, os clientes serão informados por e-mail ou no painel de autosserviço.