Questionário de Segurança e Privacidade da Informação

A CentralServer publica o presente questionário, que trata das práticas e procedimentos adotados pela empresa para proteger a segurança e a privacidade de dados ao fornecer acesso a recursos computacionais para colaboradores, clientes e fornecedores, devidamente autorizados, segundo padrões internacionais de gestão e em consonância com a legislação vigente.

INTRODUÇÃO	
Quais os modelos de serviços oferecidos pela CentralServer?	IaaS, CloudOps, Email.
Quais os ambientes de computação suportados pela CentralServer?	Infraestrutura e operação de virtualização com tecnologia KVM em data center. Operação das nuvens públicas Amazon Web Services (AWS) e Microsoft Azure.
Qual a terminologia dos serviços oferecidos pela CentralServer?	**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. **Virtualização KVM:** serviço de servidores virtuais da CentralServer baseado em infraestrutura de data center Ascenty, tecnologia KVM e painéis de autosserviço para provisionamento, controle e monitoramento de recursos.

INFRAESTRUTURA DO DATA CENTER	
Qual a classificação de disponibilidade dos data centers utilizados pela empresa?	Estrutura Ascenty certificada padrão Tier III, zonas de proteção contra incêndios, sistemas redundantes de energia (2N) e ar condicionado (N+20%).
Quais as normas e certificações dos data centers utilizados pela empresa?	A Ascenty segue padrões internacionais de referência para a estrutura de data center, conforme informado em: https://ascenty.com/data-centers/seguranca-e-certificacoes/certificacoes/ O KVM é um software open--source mantido pela comunidade conforme descrito em: https://www.linux-kvm.org

	A CentralServer segue o padrão NIST de Segurança para Tecnologias de Virtualização. Algumas das recomendações do guia são oferecidas aos clientes como funcionalidades opcionais.
Em qual localidade está localizado o data center?	São Paulo (Data Centers Ascenty).
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 KVM.
A infraestrutura possui escalabilidade horizontal e vertical?	Sim, com base na tecnologia de virtualização.
A infraestrutura faz uso de balanceadores de carga para distribuição em múltiplos servidores?	Funcionalidade disponível (opcional).

CONTINUIDADE DE NEGÓCIOS	
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).
Os backups estão criptografados?	Criptografia de dados armazenados disponível (opcional).
Por quanto tempo os backups são armazenados?	Período de retenção de dados de backup disponível em dias, meses ou anos (opcional).
Quais as formas de backup disponíveis?	KVM: backup realizado via ferramenta da plataforma em storages separados dos clusters de produção (opcional). AWS e Azure: backup realizado via snapshots de volumes de disco em object storage (opcional). A taxa de restauração dos backups de dados é de 200 GB/hora (ex. um disco de 400 GB leva cerca de 02 horas para ser restaurado).
Qual o mecanismo disponível para recuperação de desastres?	Uso das nuvens alternativas os data centers distintos para implantação de plano de recuperação de desastres e continuidade de negócios. Os testes de recuperação são semanais, trimestrais ou semestrais dependendo do tipo de sistema. (opcional no caso de clientes).
Qual o tempo necessário para a recuperação dos serviços em caso de desastre?	15 a 240 minutos, conforme o projeto (opcional no caso de clientes).

Qual a periodicidade de realização de testes de recuperação de desastres?	Trimestral ou semestral (opcional no caso de clientes).

MONITORAMENTO DE RECURSOS	
Como são monitorados os recursos do data center?	KVM: 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.
Como são monitoradas as máquinas virtuais, servidores web, bancos de dados e demais aplicações?	KVM: através de sistema de monitoramento nativo da plataforma e, opcionalmente, através 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	
Como funciona a segurança física do data center?	KVM: 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 ocorrer mudança de pessoal. Sistema de eclusa na portaria, porta controlada na recepção e detector de metais. O 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.
Qual o sistema de proteção contra incêndio utilizado no data center?	KVM: sistema de proteção contra incêndios com gás FM-200. AWS e Azure: proteção de incêndio implantada pelos respectivos fornecedores.
Qual o procedimento de descarte seguro dos dados existentes nos diferentes tipos de mídia?	KVM: recolhimento para laboratório de mídias como: flash-drive, CD/DVD, HDD, SSD e papel; desmontagem, inutilização e descarte para reciclagem. AWS e Azure: procedimento executado pelos respectivos fornecedores.
A empresa possui procedimento de controle de acesso físico ao data center?	Procedimentos de controle de acesso implantados para garantir que somente pessoas autorizadas tenham acesso ao data center (instalações prediais e área de servidores).

SEGURANÇA LÓGICA	
O acesso à rede do data center é protegido por firewalls?	Firewalls multicamadas redundantes com funções stateless e stateful usadas para proteção da rede.
Como são protegidos os acessos remotos aos sistemas da infraestrutura?	KVM: 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.
Como é feita a proteção da rede contra ataques?	KVM: 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.
Há sistemas para proteção contra vírus e intrusos?	Uso de sistemas antivírus e de detecção de intrusão disponíveis a nível de infraestrutura e sistema operacional de servidores, notebooks e desktops (opcional no caso de clientes).

A empresa possui filtros para envio e recebimento de email pelos colaboradores?	Uso de filtros para mitigar riscos de segurança relacionados ao envio e recebimento de emails dos colaboradores.
A empresa é capaz de detectar incidentes de segurança, como: acesso não autorizado, destruição, perda, alteração e vazamento de dados?	Uso de sistemas para detectar e responder a incidentes de segurança que possam comprometer a autenticidade, confidencialidade e privacidade de dados, de acordo com as possibilidades técnicas.
A empresa possui processo de registro de notificações que tenha recebido em relação a incidentes de segurança?	Plano de Resposta a Incidentes de Segurança que inclui as etapas de: registro (data/hora, fonte da notificação, tipo e descrição do incidente), análise (riscos ou impactos), contenção, comunicação, investigação, medidas corretivas, revisão e melhoria contínua.
Como é feito o isolamento de recursos entre os clientes do data center?	KVM: segmentações físicas e lógicas de rede (vlans). Controle de ARP para proteção anti-spoofing. Disponibilidade de firewall de rede para isolamento de máquinas virtuais. AWS e Azure: isolamento de recursos implantado por mecanismos específicos de cada fornecedor.
A empresa faz hardening em sistemas operacionais de servidores e bancos de dados?	Procedimento de hardening existente para os sistemas operacionais e bancos de dados gerenciados.
A empresa faz varredura periódica de vulnerabilidades nos sistemas?	Varreduras diárias nos servidores e testes regulares de rede para identificação de vulnerabilidades.
A empresa utiliza conexões seguras (TLS/HTTPS) ou aplicativos com criptografia fim-a-fim para serviços de comunicação?	Uso de conexões seguras HTTPS/TLS para acesso aos serviços web e email. Uso de criptografia fim-a-fim quando disponibilizado pelos fornecedores das aplicações.
A empresa suporta criptografia de dados em repouso (encryption at rest)?	Fornecida opção de criptografia de dados em repouso para os sistemas operacionais Linux e Windows Server.
A empresa faz testes de segurança (pentest) no seu site e sistemas?	A CentralServer faz testes de segurança no seu site e sistemas com frequência mensal.
A empresa possui rede sem fio (wi-fi) corporativa e para visitantes?	Fornecida rede sem fio (wi-fi) aos colaboradores para acesso à internet pública. É proibido o acesso de visitantes à rede wi-fi e à rede corporativa.

OPERAÇÕES	
Como são tratadas as solicitações de serviços?	Abertura de chamados via Portal de Suporte, console de autosserviço ou aplicativo de mensagem por usuários previamente cadastrados no console de autosserviço.
Os procedimentos operacionais são documentados e controlados?	Procedimentos operacionais documentados, revisados regularmente e organizados em base de conhecimento acessível pela equipe interna.
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.

Como são realizados os procedimentos de manutenção e mudança de equipamentos e sistemas?	Manutenções que envolvam inatividade de serviços, possibilidade de impacto não planejado ou risco de perda de dados realizadas via processo de Gestão de Mudança (GMUD). As mudanças são registradas em uma ferramenta específica e divulgadas para todas as partes interessadas (stakeholders internos e externos). O procedimento envolve: avaliação de risco e impacto, abertura de janela de manutenção, comunicados aos stakeholders e procedimento de reversão.
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 dos 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 e os órgãos reguladores são informados a respeito dos incidentes e das ações tomadas por meio de notificações e pareceres técnicos.
Existe a separação dos recursos de desenvolvimento, teste e produção?	Ambientes de desenvolvimento, teste e produção dos sistemas devidamente implantados.
Como funciona o controle de versões de software e a aplicação de correções de segurança?	KVM: uso de repositórios Git para versionamento do console de autosserviço e sistemas de gestão. Controle de versão e aplicação de atualizações da infraestrutura pelo gerenciador da plataforma. 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 TI	
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. A política é avaliada e auditada periodicamente pelo Comitê de

	Segurança e Privacidade da Informação. Aborda temas relevantes relacionados à proteção de dados, como Senhas, Controle de Acesso, Gestão de Incidentes, Backups, Comunicação, Acesso e Comportamento na Internet, Privacidade, Testes de Segurança, Transferência de Informações, Registro e Auditoria de Eventos, Auditoria, Descarte e Destruição de Informações, entre outros.
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 que têm acesso a dados e sistemas da empresa.
Existe um processo de análise de riscos e formas definidas de mitigação de problemas de segurança?	Comitê interno de Segurança e Privacidade da Informação para análise de riscos e impactos sobre segurança e privacidade com reuniões mensais ou em caráter extraordinário quando necessário.
A equipe recebe treinamentos periódicos de boas práticas de segurança da informação e privacidade de dados?	Treinamentos dos novos colaboradores e reuniões regulares com a equipe para apresentação de normas e orientações sobre boas práticas de segurança da informação e privacidade de dados.
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.
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.
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 em períodos de até 60 dias.
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. Uso de 2FA nos demais sistemas utilizados pela empresa sempre que disponível.
A empresa possui ferramentas para administração de solicitações de IT?	Uso de ferramenta de ITSM para envio e controle de solicitações de TI, incluindo autorizações de acesso mediante aprovação.
A empresa faz bloqueio de acesso do colaborador que está em período de férias ou em licença?	Bloqueio dos acessos à rede interna de colaboradores que estão em férias ou licença para evitar possíveis brechas de segurança.
A empresa faz bloqueio de acesso de colaboradores que encerram o contrato de trabalho?	O bloqueio dos acessos é realizado antecipadamente para usuários com acesso a sistemas críticos Para os demais, em até 2 horas após o encerramento do contrato de trabalho.

A empresa possui processo de revisão de permissões de acessos aos sistemas de tecnologia?	Revisão semestral, ou em menor período quando necessário, das permissões de acesso aos sistemas críticos ou que contenham dados pessoais.
A empresa possui os papéis e responsabilidades de Segurança da Informação definidas?	Comitê de Segurança e Privacidade da Informação (CSPI) estabelecido e com normas definidas para orientar suas atividades, equipe técnica especializada em segurança de TI e colaboradores treinados sobre suas responsabilidades quanto à segurança da informação.
A empresa define e comunica ações disciplinares a que estão sujeitos colaboradores que violem as determinações de Segurança da Informação?	Sanções cabíveis aos colaboradores que venham a infringir as normas de Segurança da Informação são definidas e divulgadas.
A empresa faz gestão de vulnerabilidades técnicas identificadas em sistemas?	Acompanhamento automatizado e manual das divulgações de correções de segurança (patches) de fornecedores, instalação de patches e monitoramento de sistemas para gestão de vulnerabilidades técnicas.
A empresa possui inventário dos ativos associados com segurança da informação?	Inventário e controle dos ativos associados à segurança da informação realizado regularmente (Desktops, Notebooks, Servidores, Componentes de Redes, etc.)
A empresa possui um plano para atualização de software dos equipamentos e sistemas nos notebooks, desktops, servidores, bancos de dados, etc.)?	Procedimento existente para atualização regular de firmware, sistemas operacionais e aplicações.
A empresa permite gravar dados em mídias removíveis (flash-drive, CD/DVD, HD externo, etc.)?	É bloqueado acesso de leitura e escrita em mídias removíveis em desktops, notebooks e servidores.
A empresa utiliza ambientes de Produção, Homologação e Testes para sistemas desenvolvidos ou adquiridos de terceiros?	Uso de ambientes de Produção, Homologação e Testes para os sistemas utilizados internamente pela empresa.
Na empresa, a identificação e autenticação do usuário na rede e em sistemas de tecnologia é individual?	Uso de autenticação individual baseada em Active Directory, LDAP e sistemas Single Sign-On (SSO) para garantir a segurança dos acessos aos sistemas de tecnologia.
A empresa possui uma política de desenvolvimento seguro de código?	A CentralServer possui uma política de desenvolvimento seguro de código que é revisada regularmente.
Como a empresa analisa a qualidade e segurança dos códigos produzidos?	A empresa utiliza metodologias de análise de qualidade de códigos para garantir que os sistemas sejam seguros e livres de vulnerabilidades.
A empresa fornece treinamentos de desenvolvimento seguro para os desenvolvedores?	Disponibilidade de treinamentos para desenvolvedores de códigos com o objetivo de garantir que o desenvolvimento seguro seja uma prática comum.
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, exceto quando este registro é impossibilitado pelo fabricante.

PRIVACIDADE DE DADOS	
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/
A empresa possui um programa institucional de Privacidade de Dados?	Programa de Privacidade e Proteção de Dados implantado, que atende às exigências da LGPD e está em conformidade com a legislação vigente.
Ao desenvolver novos produtos, serviços e projetos, a privacidade é levada em consideração?	Utilizamos a abordagem de privacy by design e privacy by default no desenvolvimento de seus produtos, serviços e projetos, visando garantir a privacidade dos dados pessoais.
A empresa possui um Encarregado - DPO (Data Protection Officer) nomeado e divulgado de forma facilitada e clara?	Encarregado pelo tratamento de dados pessoais (DPO) nomeado e com contato divulgado na página: https://www.centralserver.com/br/politica-de-privacidade/
Os contratos ou Aditivos de trabalho com colaboradores possuem cláusulas compatíveis com a LGPD?	Contratos e aditivos de trabalho dos colaboradores da CentralServer com cláusulas compatíveis com a LGPD.
A empresa possui Registro das Operações de Tratamento de Dados Pessoais?	Registros de mapeamento, fluxos de dados e das operações de tratamento de dados pessoais existentes.
A empresa identifica as bases legais, de acordo com a LGPD, para coleta e tratamento de dados?	Bases legais identificadas para coleta e tratamento de dados conforme documentado na nossa Política de Conformidade com a LGPD.
A empresa, quando cabível, obtém o consentimento prévio e documentado do titular dos dados pessoais para realizar qualquer tipo de tratamento?	Consentimento prévio e documentado do titular dos dados pessoais quando cabível, para realizar o tratamento de dados pessoais.
Caso haja alteração na finalidade do tratamento de dados pessoais, a empresa possui procedimento para informar aos titulares dos dados pessoais acerca desta mudança e obter novo consentimento, se necessário?	Processo existente para informar aos titulares sobre alterações na finalidade do tratamento de dados pessoais e obter novo consentimento, quando necessário.
A utilização do legítimo interesse como base legal para a coleta e processamento de dados (se houver) é aplicada mediante a realização do teste de proporcionalidade?	Procedimento de análise da proporcionalidade e fundamentação da coleta e processamento de dados pessoais com base no legítimo interesse do controlador realizado.
A empresa possui procedimentos para atender aos direitos do titular, incluindo a comunicação	Procedimentos existentes para atender aos direitos dos titulares de dados, incluindo o direito de acesso, retificação, exclusão,

aos agentes de tratamento com os quais tenha compartilhado dados para que repitam tal procedimento?	portabilidade e oposição tanto internamente quanto junto aos agentes de tratamento com quem compartilha dados pessoais, exceto quando esta comunicação seja impossível ou implique em esforço desproporcional.
A empresa define e comunica ações disciplinares a que estão sujeitos colaboradores que violem as determinações de Privacidade da Informação?	Sanções cabíveis aos colaboradores que venham a infringir as normas de Privacidade da Informação são definidas e divulgadas.
A empresa possui procedimentos para retificar ou eliminar dados pessoais de todos os seus sistemas e bancos de dados, se necessário?	Procedimentos existentes para retificar ou eliminar dados pessoais em seus sistemas e bancos de dados, caso necessário e cabível perante a legislação. Adicionalmente, os bancos de dados são revisados regularmente para eliminar dados desnecessários e anonimizar dados pessoais.
A empresa possui processo apropriado para notificar os titulares sobre um incidente envolvendo dados pessoais, quando aplicável?	Processo para notificar os titulares de dados em caso de incidentes de segurança que afetem seus dados pessoais existentes
A empresa confecciona o Relatório de Impacto à Proteção de Dados Pessoais para atividades de tratamento que resultem em um alto risco para os titulares?	Procedimentos existentes para avaliar se uma atividade de tratamento de dados apresenta risco aos direitos e liberdades dos titulares e, em caso afirmativo, elaborar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD).
A empresa realiza tratamento de dados pessoais de crianças e adolescentes?	Não.
Em casos de transferência internacional de dados pessoais, há cláusulas contratuais de privacidade e proteção de dados em seus contratos?	Possuímos cláusulas contratuais de privacidade e proteção de dados em seus contratos de transferência internacional de dados pessoais, conforme exigido pela LGPD.
O site da empresa apresenta a Política de uso de Cookies?	Política de Cookies publicada no site da empresa.
A empresa adota práticas para remover dados pessoais que estejam desnecessariamente disponibilizados em redes públicas?	Política de segurança existente que estabelece a responsabilidade dos colaboradores em proteger e controlar os dados pessoais publicados em redes públicas.
A empresa possui metodologia para graduação e gestão de Riscos de Segurança da Informação e Privacidade?	Metodologia para graduação de riscos de segurança e privacidade da informação existente. Política de Segurança da Informação e Norma de Gestão de Riscos de TI para a devida gestão de riscos de segurança da informação.

TERMOS DE USO

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/

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.