SCGÁS COMPANHIA DE GÁS DE SANTA CATARINA	GETIN - Gerência de Tecnologia da Informação
	Memorial Descritivo
	Soluções de Controle de Acesso e Autenticação Centralizada

Resumo: **Contratação de Soluções de Controle de Acesso e Autenticação Centralizada com suporte por um período de 60 (sessenta) meses.**

A seguir os requisitos necessários para contratação das Soluções de Controle de Acesso e Autenticação Centralizada:

1. REQUISITOS GERAIS

1.1 Todos os itens devem acompanhar 60 (sessenta) meses de suporte oficial do fabricante.
1.2 O serviço de suporte do fabricante deve prover as assinaturas, acesso ao portal de suporte e novas versões de software durante a vigência do contrato.
1.3 O SLA de atendimento para chamados considerados críticos deve ser de 1(uma) hora e para não críticos até o próximo dia útil.

2. Solução de controle de acesso à rede

2.1 Solução de controle de acesso à rede, a ser ofertado em formato de appliance físico ou virtual, este que deverá estar disponível para as plataformas VMware ESXi, Hyper-V, AWS e Microsoft Azure.
2.2 Deve encaminhar os logs para a ferramenta FortiAnalyzer existente na SCGÁS;
2.3 Deve permitir colocar um dispositivo em quarentena através da integração nativa com o FortiGate 200F existente na SCGÁS.
2.4 Deve ser uma solução multi-vendor e não depender da implementação de 802.1x para o seu funcionamento.
2.5 Deve ser fornecido para 600 (seiscentos) dispositivos.
2.6 A solução deve ser entregue em alta disponibilidade.
2.7 A solução deve ser capaz de inspecionar tanto IoT quanto estações/notebooks, sem depender de recursos como 802.1X e Mac-address bypass (MAB);
2.8 Para estações de trabalho, deve suportar verificação de compliance em VPN IPsec e SSL.
2.9 A licença contemplada deverá suportar todas as características exigidas neste termo de referência.
2.10 A solução deve permitir diferentes perfis de administração, com a capacidade de limitar e controlar a quantidade de acesso permitido às funcionalidades disponíveis, dependendo do grupo administrativo da organização ao qual o usuário pertence.
2.11 Deve detectar e classificar automaticamente o tipo dos dispositivos conectados na rede sem a necessidade de softwares instalados nos dispositivos.
2.12 Deve permitir determinar o perfil dos dispositivos descobertos por meio de métodos que não exigem a instalação de agentes, incluindo pelo menos os seguintes:

2.12.1 Consultas em DHCP Fingerprint.
2.12.2 Consultas via protocolos HTTP/HTTPS.
2.12.3 Consultas via protocolo SNMP.
2.12.4 Consultas via protocolo SSH.
2.12.5 Consultas via protocolo Telnet.
2.12.6 Consultas de portas TCP.
2.12.7 Consultas de portas UDP.
2.12.8 MAC OUI.
2.12.9 Consultas via protocolo WMI.
2.12.10 Protocolo ONVIF.
2.12.11 Base assinaturas pré-definidas.

2.13 A solução deve ser capaz de reconhecer as seguintes informações sobre os dispositivos conectados à rede:
2.13.1 Endereço MAC.
2.13.2 Endereço IP.
2.13.3 Sistema operacional.
2.13.4 Nome do host.
2.13.5 Horário de conexão.
2.13.6 Usuário conectado.
2.13.7 Localização.

2.14 A solução deve ser capaz de reconhecer os seguintes sistemas operacionais em execução nos dispositivos conectados à rede:
2.14.1 Android.
2.14.2 Apple iOS para iPhone, iPod e iPad.
2.14.3 Chrome OS.
2.14.4 Linux.
2.14.5 MacOS X.
2.14.6 Windows 10 ou superior.

2.15 Deve lembrar o perfil atribuído a cada dispositivo e verificar sua validade a cada conexão.
2.16 Deve permitir a designação de um sponsor para autorizar a categorização dos dispositivos.
2.17 Deve permitir a recategorização periódica de dispositivos.
2.18 Deve permitir a importação de um arquivo CSV contendo informações sobre os dispositivos a serem registrados.
2.19 A solução deve incluir a detecção de dispositivos desconhecidos conectados à rede e adotar medidas de controle para limitar o acesso.
2.20 A solução deve suportar autenticação através de EAP-PEAP e EAP-TLS.
2.21 A solução deve suportar RADIUS Change of Authorization

Resumo: **Contratação de Soluções de Controle de Acesso e Autenticação Centralizada com suporte por um período de 60 (sessenta) meses.**

2.22 A solução deve suportar MAC Address Bypass
2.23 A solução deve consultar bases LDAP e Active Directory para a identificação de usuários e grupos de usuários.
2.24 A solução deve permitir a criação de políticas de controle que combinem informações sobre a identidade do usuário e tipo de dispositivo com objetivo de autorizar dinamicamente o acesso à rede.
2.25 Deve permitir a definição dos horários em que os dispositivos serão autorizados a conectar na rede.
2.26 Deve garantir a segmentação dinâmica da rede e aplicação de políticas de segurança, tendo como base variadas combinações, como login do AD e atributos (departamento, cidade, e-mail, telefone), características da máquina (asset tag, hostname), localidade e horário.
2.27 A solução deve incluir recursos de gerenciamento de visitantes, permitindo a criação de diferentes perfis de utilização e autorização a serem associados aos usuários, distinguindo por exemplo prestadores de serviços dos visitantes.
2.28 A solução deve permitir o cadastro dos usuários visitantes na base interna da ferramenta para que não seja necessário realizar consultas em bases externas.
2.29 A solução deve possuir ferramenta que permita a geração automática de credenciais para usuários visitantes com login e respectivas senhas.
2.30 A solução deve possuir ferramenta que permita a criação de credenciais para eventos.
2.31 Deve permitir a definição de complexidade da senha dos usuários visitantes.
2.32 Deve ser possível definir um período de validade para as contas de usuários visitantes.
2.33 Deve ser possível definir data e horário para início e encerramento das contas de usuários visitantes.
2.34 A autenticação e autorização dos usuários visitantes deve ocorrer através de portal captivo acessível via browser web.
2.35 Os visitantes em hipótese alguma deverão ter acesso à Internet e rede interna antes que a autenticação seja concluída e o usuário seja autorizado.
2.36 A solução deve vincular o login do visitante à máquina utilizada no acesso.
2.37 Deve suportar a validação de credenciais:
- 2.37.1 Em base local interna à ferramenta.
- 2.37.2 Em servidores RADIUS.
- 2.37.3 Em servidores LDAP.

2.38 A solução deve autenticar usuários visitantes através das seguintes redes sociais: Facebook, LinkedIn e Twitter.
2.39 A ferramenta deve permitir que os usuários visitantes possam realizar auto registro através do preenchimento de cadastro disponível em portal web.

Resumo: **Contratação de Soluções de Controle de Acesso e Autenticação Centralizada com suporte por um período de 60 (sessenta) meses.**

2.40 Deve permitir a customização dos campos obrigatórios e opcionais para o cadastro de auto registro.
2.41 A solução deve suportar o envio da senha de acesso aos visitantes através de SMS e e-mail.
2.42 Deve ser possível definir um período para que os usuários visitantes sejam obrigados a se reautenticar.
2.43 Deve permitir a designação de grupos de usuários com função de sponsor que ficarão responsáveis por autorizar o acesso dos usuários visitantes e prestadores de serviços.
2.44 Os usuários do tipo sponsor poderão cadastrar previamente um usuário visitante. O portal de cadastro e gerenciamento de usuários visitantes não deve permitir gerência administrativa dos demais recursos da solução.
2.45 A solução deve permitir a customização da aparência do captive portal, permitindo editar textos e inserir imagens.
2.46 Os usuários do tipo sponsor podem ser cadastrados na base local da ferramenta ou fazer parte de grupo de usuários em base LDAP/Active Directory.
2.47 A solução deve incluir recursos de conformidade de endpoint. Antes de permitir que os dispositivos acessem a rede, a solução deve garantir que estes cumpram requisitos de segurança, integridade e conformidade.
2.48 Deve permitir o uso de software agente instalado no dispositivo e agentes evanescentes que não precisam ser instalados.
2.49 Tanto para IoTs quanto para estações de trabalho, se configurado, não devem ter qualquer acesso à rede de produção enquanto não forem inspecionados e identificados.
2.50 Se um dispositivo não passar os testes de conformidade, deve ser possível:
- 2.50.1 Não forçar a remediação.
- 2.50.2 Forçar a remediação imediatamente enviando o dispositivo à rede de quarentena;
- 2.50.3 Permitir a remediação retardada, ou seja, dando um período de tolerância para que o usuário corrija o problema. Caso os problemas persistam, o dispositivo deve ser colocado em quarentena.

2.51 A solução deve permitir verificações de conformidade em endpoint que façam uso do sistema operacional:
- 2.51.1 Windows 10 ou superior.
- 2.51.2 MacOS.
- 2.51.3 Linux.

2.52 Para garantir a conformidade com as políticas de segurança, a solução deve permitir que sejam verificados os seguintes itens antes de autorizar o acesso de um endpoint na rede:
- 2.52.1 Presença de software de antivírus instalado e em execução.

2.52.2 Versão do sistema operacional.
2.52.3 Nome de domínio do Active Directory ao qual a estação Windows pertença;
2.52.4 Serviços em execução para estações Windows.
2.52.5 Informações sobre um determinado certificado digital em estações Windows.
2.52.6 Registros ou chaves de registro para estações Windows.
2.52.7 Processos em execução para estações Windows, Linux e MacOS.
2.52.8 Arquivo armazenado em um determinado diretório para estações Windows, Linux e MacOS.
2.52.9 Pacotes instalados em estações Linux e MacOS.

2.53 A solução deve ser capaz de monitorar quando um serviço requirido for desabilitado ou interrompido em computadores. Além disso deve enviar a estação para quarentena de forma a garantir a conformidade com a política de segurança.

2.54 Deve possuir serviço RADIUS interno, além de permitir o uso de RADIUS externos.

2.55 Deve permitir a distribuição de agentes através de, pelo menos, os seguintes métodos:

2.55.1 Programas de gerenciamento e distribuição de software.
2.55.2 GPO do Active Directory.
2.55.3 Captive Portal.

2.56 Deve permitir a atualização automática ou programada dos agentes instalados nas máquinas.

2.57 O agente instalado nos computadores deve notificar os usuários com mensagens informativas em casos de eventos.

2.58 Quando em quarentena, um portal web deve ser apresentado aos usuários com informações sobre as razões pelas quais estes foram movidos para o isolamento.

2.59 A solução deve compartilhar a identificação dos usuários e/ou dispositivos autenticados para a plataforma de segurança da rede via SSO, de forma que sejam vinculadas aos acessos de Internet, provendo rastreabilidade futura.

2.60 No que tange compliance, quando houver sucesso, falha ou alerta, a solução deve permitir as seguintes ações: alerta, envio de e-mail e SMS, desabilitar o host, envio de mensagem direta para o host envolvido e executar políticas adicionais de compliance.

2.61 A solução deve integrar com plataformas de MDM, suportando pelo menos: FortiClient, In Tune, Mobile Iron e Air Watch.

2.62 A solução deve possuir dashboard que apresente informações e estatísticas relevantes de forma resumida.

2.63 A solução deve permitir a customização do dashboard para apresentar as informações que o administrador considera relevante.

Resumo: **Contratação de Soluções de Controle de Acesso e Autenticação Centralizada com suporte por um período de 60 (sessenta) meses.**

2.64 A solução deve permitir a consulta de informações e alteração de parâmetros de configuração via REST API.
2.65 A solução deve armazenar os eventos internamente e permitir que sejam exportados.
2.66 Deve ser fornecido em alta disponibilidade, suportando todos os registros e autenticações caso um nó da solução esteja indisponível.
2.67 A solução deve ser capaz de isolar hosts na quarentena mesmo quando estes estão conectados em redes de localidades remotas, tais como filiais. Não deve ser necessário estender a VLAN para isso.
2.68 Deve possuir registro dos eventos ocorridos na solução, bem como auditoria das configurações efetuadas.
2.69 Deve possibilitar o rastreio de dispositivos, notificando a localização deles quando se conectarem à rede.
2.70 Dentre os relatórios disponibilizados pela solução dedicada de logs, deve suportar relatórios listando os endpoints por localidade e fabricante, usuários associados, além de relatórios de inventário, devices registrados e rogues.
2.71 O contratado deverá implementar e configurar a solução garantindo no mínimo:

- O Download das OVFs e deploy com setup de conectividade básico das VMs
- Configuração de alta disponibilidade
- Integração com o AD
- Criação dos grupos e políticas para autenticação via RADIUS
- Criação de políticas de autenticação das redes cabeadas e wireless
- Criação de políticas de autenticação através de MAB para os dispositivos sem possibilidade de autenticação
- Criação de políticas de profiling

3. Solução de autenticação centralizada

3.1 Deve possuir licenciamento para 400 (quatrocentos) usuários locais ou remotos concorrentes, com suporte por 36 meses.
3.2 Deve incluir todos os recursos e licenciamento para funcionar em alta disponibilidade (ao menos 2 instâncias).
3.3 Deve suportar administração em interface gráfica (GUI) por HTTP e/ou HTTPS.
3.4 Deve suportar administração em interface baseada em linhas de comando (CLI) por TELNET e/ou SSH.
3.5 Deve permitir definir perfis de administradores para a solução, de modo que possa segmentar a responsabilidade dos administradores por tarefas operativas.

Resumo: **Contratação de Soluções de Controle de Acesso e Autenticação Centralizada com suporte por um período de 60 (sessenta) meses.**

3.6 Deve possuir Indicador visual, centralizado, de informações críticas (estado da licença, versão de firmware, consumo de CPU/Memória/Disco, quantidade de usuários criados e licenciados).
3.7 Deve suportar a atualização do firmware via interface gráfica, por processo simplificado e intuitivo.
3.8 Deve suportar customização de mensagens padrão da solução como páginas de erro, portais de autenticação, auto registro, reset de senha e outros. Suportar também a inclusão, alteração e remoção de imagens nas mensagens/páginas sem a necessidade de recursos ou conectividade externa.
3.9 Deve suportar configuração de Alta Disponibilidade (HA), reduzindo ao máximo os períodos de interrupção.
3.10 Deve suportar implementações de HA como "Ativo-Passivo" ou sincronizando configurações entre duas caixas ativas.
3.11 Deve permitir sincronismo automático de configurações entre todos os equipamentos que componham a solução em HÁ.
3.12 Deve suportar implementação de HA sincronizando configurações com appliances em localidades geograficamente separadas.
3.13 Deve suportar a opção de backup criptografado.
3.14 Deve suportar backup automatizado (agendados por critérios pré-definidos), não somente sob demanda.
3.15 Deve suportar o backup completo da configuração, incluindo base de usuários, grupos, tokens, certificados, configurações de single-sign-on. A solução deve também permitir a restauração de toda configuração diretamente da interface gráfica.
3.16 Deve suportar NTP (Network Time Protocol), visando o sincronismo de hora/data.
3.17 Deve suportar SNMP v1, v2 e v3 permitindo consultar MIB própria e envio de Traps.
3.18 Deve suportar nativamente Trap SNMP indicando mudança de status de HA.
3.19 Deve suportar captura de pacotes através da interface gráfica para Troubleshoot avançado em ferramentas de análise de pacotes (ex.: Wireshark).
3.20 O equipamento deve permitir o envio de e-mails relacionados a reset de senha, aprovação de novos usuários, auto-registro de usuários e autenticação de segundo fator (token).
3.21 Deve suportar o registro de todos os eventos que os usuários de sua base de dados local realizem com suas contas, tais como criação de um usuário, troca de senha de um usuário e alteração de informação gerais.
3.22 AUTENTICAÇÃO
    3.22.1 A solução deve efetuar autenticação para a gerência de identidade dos usuários da rede, ajudando a simplificar a administração deles sendo um ponto

Resumo: **Contratação de Soluções de Controle de Acesso e Autenticação Centralizada com suporte por um período de 60 (sessenta) meses.**

central de controle de autenticação, onde múltiplos métodos de autenticação possam ser consolidados.
3.22.2 Deve suportar autenticação em dois fatores (two-factor authentication).
3.22.3 Deve possuir suporte a autenticação de dois fatores em pelo menos dois tipos diferentes de tokens, sendo o primeiro físico (token), e o segundo lógico como software para dispositivos móveis, e-mail ou SMS, permitindo que seja dada a escolha de qual dos tipos utilizar para cada usuário. Tokens e licenciamento de SMS não inclusos nesta especificação.
3.22.4 Deve permitir que se defina um perfil de complexidade mínimo para as senhas de todos os usuários cadastrados na base de dados local, possibilitando a definição de número mínimo de letras minúsculas, letras maiúsculas, caracteres numéricos, caracteres especiais etc.
3.22.5 Deve permitir a criação de política de bloqueio automático de usuários após uma quantidade de falhas de autenticação, assim evitando ataques de força bruta.
3.22.6 Deve suportar a criação de usuários em base local, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade.
3.22.7 Deve permitir a criação em massa de usuários na base de dados local através da importação de lista de usuários a serem criados contida em arquivos externos.
3.22.8 Deve permitir a criação de novos usuários na base de dados local e que o criador/administrador possa definir uma senha no momento de criação.
3.22.9 Deve permitir a criação de novos usuários na base de dados local de forma que o equipamento gere uma senha aleatória e envie automaticamente ao usuário.
3.22.10 Deve permitir a criação de novos usuários na base de dados local sem a definição de senha, exigindo que ele utilize o token como único fator de autenticação.
3.22.11 Deve permitir associar os tokens aos usuários criados localmente na base de dados.
3.22.12 Deve permitir que os próprios usuários façam o registro dos seus tokens e relatem a perda de um token automaticamente, sem necessidade de envolver um administrador.
3.22.13 Deve permitir remoção automática em massa de usuários desabilitados, baseado em critérios definidos.
3.22.14 Deve possuir formas que permitam que os usuários locais possam fazer o reset de suas senhas de forma segura sem a intervenção de administradores, através de correio eletrônico ou pergunta de segurança.

Resumo: **Contratação de Soluções de Controle de Acesso e Autenticação Centralizada com suporte por um período de 60 (sessenta) meses.**

3.22.15 Deve suportar a criação de grupos de usuários, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade.
3.22.16 Os tokens devem gerar códigos com no mínimo 6 dígitos e intervalos não superiores à 60 segundos.
3.22.17 Deve suportar autenticação em dois fatores por hardware dedicado (Token).
3.22.18 Deve suportar autenticação em dois fatores por aplicativo mobile (iOS e Android).
3.22.19 Deve suportar autenticação em dois fatores por envio de e-mail.
3.22.20 Deve suportar a sincronização com dispositivo em hardware de geração de OTP (One Time Password).
3.22.21 Deve permitir sincronizar os tokens com o equipamento para o correto funcionamento dos mesmos.
3.22.22 Deve permitir desabilitar um token quando este seja roubado ou extraviado, permitindo sua reativação posterior quando/se for recuperado.
3.22.23 Deve permitir a desassociação de um token a um usuário e associá-lo a outro usuário quando necessário, permitindo assim que sejam reaproveitados.
3.22.24 Deve continuar permitindo a autenticação de dois fatores em clientes windows mesmo com a máquina offline.
3.22.25 Deve prover um portal web para o auto-registro dos usuários, de forma que o mesmo acesse, preencha os seus dados e submeta o registro. Após o usuário efetuar o registro, o administrador deverá ser notificado automaticamente para aprovar ou negar o cadastro do mesmo antes de que ele seja ativado.
3.22.26 Deve funcionar como servidor RADIUS (Remote Authentication Dial-In User Server), proporcionando autenticação aos dispositivos compatíveis com tal protocolo.
3.22.27 Deve suportar a integração com servidor RADIUS remoto.
3.22.28 Deve ter capacidade de funcionar como servidor LDAP (Lightweight Directory Access Protocol), proporcionando autenticação aos dispositivos compatíveis com tal protocolo.
3.22.29 Deve suportar a integração com servidor LDAP remoto (como Microsoft Active Directory).
3.22.30 Deve suportar autenticação de usuários com credenciais de mídias sociais de terceiros como Facebook, Twitter, LinkedIn e Google+.
3.22.31 Deve permitir que usuários que não possuam uma conta local ou em mídias sociais se autentiquem através de um rápido cadastro, que garanta o mínimo de rastreabilidade, através da validação de endereços de e-mail ou número de telefone.

3.22.32 Deve permitir o login automático de usuários visitantes depois de se registrarem com sucesso.
3.22.33 Deve permitir configurar os parâmetros de rede (como as configurações de WiFi) em um endpoint baixando um script ou um executável através do portal de visitantes.
3.22.34 Deve suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Indentity Provider - IDP) estabelecendo um relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider -SP).
3.22.35 Deve permitir integração com bases do Azure Directory e Gsuite.
3.22.36 Por meio do SAML, deve permitir integrações com SPs variados, tais como Office 365.

3.23 CERTIFICADOS

3.23.1 Deve atuar como Autoridade Certificadora (CA).
3.23.2 Deve permitir a administração de certificados digitais, com emissão e revogação.
3.23.3 Deve permitir o uso de CA's confiáveis para validação de certificados emitidos por CA's externas.
3.23.4 Deve suportar OCSP para que se possa fornecer uma lista de certificados revogados (CRL).
3.23.5 Deve prover repositório para autenticação de VPN Site-to-Site através de Certificados.
3.23.6 Deve suportar SCEP Server (Simple Certificate Enrollment Protocol), permitindo a assinatura de requisições de certificados digitais (CSR) automaticamente ou com interação do administrador.
3.23.7 Deve ser capaz de importar outros certificados de CA's assim como a lista de certificados revogados.
2.23.8 Deve ser capaz de permitir ao administrador do sistema gerar, assinar e revogar certificados digitais para os usuários.

3.24 SERVIÇO DE AUTENTICAÇÃO ÚNICA (SINGLE SIGN-ON)

3.24.1 Deve prover capacidade de serviço SSO (Single Sign-On), com autenticação transparente (passiva) de usuários em sistemas compatíveis.
3.24.2 Deve ser capaz de integrar-se a um diretório ativo (Windows AD) e poder oferecer a funcionalidade se SSO, onde a autenticação automática/transparente via SSO para os serviços necessários é baseada na autenticação prévia feita pelo usuário no domínio.

Resumo: **Contratação de Soluções de Controle de Acesso e Autenticação Centralizada com suporte por um período de 60 (sessenta) meses.**

3.24.3 Deve permitir definir uma lista de usuários de SSO que serão ignorados, evitando assim interferência de contas de serviços tais como antivírus ou scripts via GPO.
3.24.4 Deve suportar análise de arquivos syslog enviados de fonte remota, para uso pelo serviço de SSO.
3.24.5 Deve suportar Security Assertion Markup Language (SAML), agindo como autenticador de um Provedor de Serviços (Service Provider - SP) solicitando informações de identidade de usuários a Provedores de Identidade (Indentity Providers - IDP's) de terceiros.
3.24.6 Deve suportar SSO baseado em Radius (RSSO - RADIUS Single Sign-On).
3.24.7 Deve suportar RSSO Accounting Proxy permitindo a recepção de pacotes radius de accouting, a modificação destes pacotes e o encaminhamento deles para vários outros pontos.

3.25 O contratado deverá implementar e configurar a solução garantindo no mínimo:

- O Download das OVFs e deploy com setup de conectividade básico das VMs
- Configuração de alta disponibilidade
- Integração com o AD
- Criação dos grupos e políticas para autenticação via RADIUS
- Criação de portal de visitantes com auto-registro + customização de mensagens

4. OBRIGAÇÕES DO CONTRATADO:

4.1 O CONTRATADO deverá fornecer os hardwares, softwares e executar os serviços conforme especificações deste Memorial Descritivo e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade especificadas neste Memorial Descritivo.
4.2 Responsabilizar-se pelos danos causados diretamente à Administração da SCGÁS ou a terceiros, decorrentes de sua culpa ou dolo, não excluindo ou reduzindo essa responsabilidade, quando da fiscalização ou o acompanhamento pela SCGÁS.
4.3 Prestar todos os esclarecimentos que forem solicitados pela SCGÁS, obrigando-se a atender, de imediato, todas as reclamações a respeito da qualidade da prestação dos serviços.
4.4 Comunicar ao gestor do contrato, por escrito, qualquer fato que não seja conforme ao objeto do contrato, para providências por parte da SCGÁS.

Resumo: **Contratação de Soluções de Controle de Acesso e Autenticação Centralizada com suporte por um período de 60 (sessenta) meses.**

4.5 Não veicular publicidade acerca da contratação, salvo prévia autorização da SCGÁS.
4.6 Manter, durante toda a vigência do contrato, todas as condições de habilitação e qualificação exigidas na licitação, conforme legislação vigente.
4.7 Todas as despesas oriundas do objeto serão de responsabilidade do CONTRATADO, como por exemplo: disponibilização de profissionais, bem como despesas de horas extras e qualquer outra aqui não mencionada.
4.8 O CONTRATADO deverá apresentar na reunião de abertura do projeto o Planejamento e Metodologia para prestação de serviços e execução do projeto.
4.9 O CONTRATADO obriga-se a zelar pela confidencialidade de qualquer informação a que, porventura, tenha acesso.
4.10 O CONTRATADO obriga-se a seguir os procedimentos definidos pela área competente, relativos à segurança da informação.
4.11 O CONTRATADO obriga-se a colaborar com a SCGÁS para a manutenção de um ambiente de dados seguro.
4.12 A SCGÁS poderá a qualquer momento executar ações de auditoria de forma presencial ou à distância.
4.13 O CONTRATADO concorda em que é responsável por ações de seus técnicos e eventuais subcontratados em tudo que diz respeito à segurança de informações.
4.14 A ocorrência de falta relacionada à segurança de informações da SCGÁS, pelo CONTRATADO e ou integrante de sua equipe, será considerada falta grave e sujeita a aplicação de penalidade, e sua recorrência poderá dar margem à rescisão unilateral do contrato, e outras ações legais cabíveis.
4.15 O CONTRATADO deverá apresentar a comprovação de vínculo com os profissionais que atenderão à SCGÁS, podendo ser empregados (apresentando cópia da ficha ou livro de registro de empregado registrado na SRT ou, cópia da Carteira de Trabalho e Previdência Social), sócio (cópia do Contrato Social devidamente registrado no órgão competente), ou contratado (cópia do contrato formal assinado pelas partes).
4.16 Executar os serviços conforme especificações deste Memorial Descritivo e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade especificadas neste Memorial Descritivo e em sua proposta.
4.17 Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.
4.18 Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078,

de 1990), ficando o CONTRATANTE autorizado a descontar dos pagamentos devidos ao CONTRATADO, o valor correspondente aos danos sofridos.
4.19 Utilizar empregados habilitados e com conhecimentos específicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor.
4.20 Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à SCGÁS.
4.21 Atender às solicitações da SCGÁS quanto à substituição dos empregados alocados, no prazo fixado pelo fiscal do contrato, nos casos em que ficar constatado descumprimento das obrigações relativas à execução do serviço, conforme descrito neste Memorial Descritivo.
4.22 Instruir seus empregados quanto à necessidade de acatar as Normas internas da Administração da SCGÁS.
4.23 Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo Contrato, devendo o CONTRATADO relatar à SCGÁS toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função.
4.24 Relatar à SCGÁS toda e qualquer irregularidade verificada no decorrer da prestação dos serviços.
4.25 Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.
4.26 Manter durante toda a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.
4.27 Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato, de acordo com o Termo de Confidencialidade disposto no Anexo do Contrato.
4.28 Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para a atividade objeto da licitação, exceto quando ocorrer algum dos eventos arrolados na Legislação em vigor.
4.29 Estar em conformidade com a Lei Nº 13.709, de 14 de agosto de 2018, a LGPD – Lei Geral de Proteção de Dados.
4.30 Executar o serviço com profissionais devidamente capacitados e de acordo com os critérios técnicos para a prestação do serviço.
4.31 Utilizar profissionais certificados no fabricante Fortinet para instalação e configuração das Soluções de Controle de Acesso e Autenticação Centralizada.

4.32 O Contratado deverá comprovar possuir profissionais certificados com no mínimo as certificações abaixo:

- FCP - FortiAnalyzer Administrator
- FCP - FortiAuthenticator Administrator
- FCSS - NSE7 Network Security

5. DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD

5.1 Para a devida garantia da privacidade e da proteção de dados pessoais, as partes comprometem-se a observar e cumprir as disposições previstas na Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), durante a execução deste Contrato e tratamento de dados pessoais decorrente deste.
5.2 As partes obrigam-se a:
5.2.1 Tratar, usar e atender os requisitos de coleta mínima necessária dos dados pessoais para os fins a que se destinam, mantendo-os registrados, organizados, conservados e disponíveis para consulta.
5.2.2 Limitar o tratamento de dados pessoais às finalidades para as quais tenham sido coletados.
5.2.3 Manter os dados pessoais armazenados apenas durante o período estritamente necessário à execução das finalidades contratuais previstas ou pelo prazo necessário ao cumprimento de eventual obrigação legal, garantindo a sua efetiva confidencialidade, bem como manter o devido armazenamento em meios seguros, preferencialmente digitais e com rastreabilidade disponível, assim como garantir destinação final segura.
5.2.4 Quando da coleta de dados pessoais sensíveis, em razão de cumprimento de obrigação acessória, armazená-los em local apartado dos demais dados pessoais e com nível de restrição ainda maior, sendo disponibilizados somente mediante requerimento formal e justificativa legítima.
5.2.5 Aplicar medidas técnicas e administrativas capazes de proteger os dados contra alteração, perda, difusão, acesso ou destruição – acidental ou intencionalmente – não autorizados ou estranhos à essa relação contratual, bem como contra qualquer outra forma de tratamento irregular.
5.2.6 Informar a outra parte imediatamente após a tomada de conhecimento caso haja alguma suspeita ou incidente de segurança concreto envolvendo dados pessoais, devendo prestar toda a colaboração necessária a qualquer investigação que venha a ser realizada.
5.2.7 Garantir que os titulares tenham acesso facilitado às informações sobre o tratamento de seus dados mediante requerimento.

5.2.8 Garantir a rastreabilidade de tratamento de tais dados durante todo o seu ciclo de vida, principalmente quanto ao download, exportação de disponibilização de documentos com dados pessoais e dados pessoais sensíveis.
5.2.9 Adotar políticas para o desenvolvimento de sistemas que incluam diretrizes de acordo com a LGPD para atendimento das necessidades de tratamento de dados pessoais.
5.2.10 Assegurar que todas as pessoas que venham a ter acesso a dados pessoais no contexto deste contrato tenham ciência e cumpram as disposições legais aplicáveis em matéria de proteção de dados pessoais.
5.2.11 Fomentar e disponibilizar treinamento e ações de conscientização relacionadas à proteção de dados pessoais e privacidade aos responsáveis pela execução do contrato, garantindo assim a implementação de Boas Práticas e da Governança, nos termos dos artigos 50 e 51 da Lei nº 13.709/2018.
5.2.12 Responsabilizar-se-á a parte que der causa a eventuais violações de dados pessoais nos termos da legislação vigente, ressalvado o direito de regresso estabelecido em lei e consideradas as circunstâncias do caso e medidas de segurança adotadas pela responsável.

6. MATRIZ DE RISCO

Identificação do Risco	Descrição	Probabilidade	Impacto	Responsável	Mitigação
Alterações na Legislação Tecnológica	Mudanças nas leis que afetam a execução e entrega do projeto.	Média	Alto	Contratante	Monitorar mudanças legislativas e ajustar requisitos conforme necessário.
Atrasos na Entrega de Requisitos	Demora na disponibilização de informações essenciais para a execução do projeto.	Alta	Médio	Contratante / Contratado	Estabelecer cronograma claro e canais de comunicação eficientes.
Atraso na entrega dos softwares / equipamentos	Demora na entrega dos softwares e equipamentos necessários para execução do projeto	Média	Alto	Contratado	Monitorar prazos de entrega e manter um plano de comunicação constante com o fornecedor.
Falhas Técnicas na execução do projeto	Problemas técnicos que comprometem funcionalidades e andamento do projeto.	Média	Alto	Contratado	Implementar testes rigorosos e revisões das etapas de execução do projeto.
Indisponibilidade de Recursos Chave	Ausência de profissionais ou ferramentas essenciais para a execução do projeto.	Baixa	Alto	Contratado	Planejamento de contingência e treinamento de equipe.

Resumo: **Contratação de Soluções de Controle de Acesso e Autenticação Centralizada com suporte por um período de 60 (sessenta) meses.**

Mudanças nos Requisitos do Projeto	Alterações significativas nos requisitos após a aprovação do cronograma e início do projeto.	Média	Alto	Contratante	Definir processo formal de gestão de mudanças e avaliação de impactos.
Problemas de Compatibilidade	Incompatibilidade com diferentes dispositivos ou sistemas operacionais.	Média	Médio	Contratado	Realizar testes abrangentes em múltiplas plataformas e dispositivos.
Falha na Integração com os sistemas existentes	Falha de integração com os sistemas existentes, principalmente com o Active Directory.	Alto	Alto	Contratado	Realizar teste de integração antecipados e ter um plano de contingência.
Resistência dos usuários à mudança	Problemas com os usuários e relação as mudanças necessárias para execução do projeto.	Média	Médio	Contratante / Contratado	Implementar um plano de gestão de mudança e comunicação eficaz.
Vulnerabilidades de Segurança não detectadas	Vulnerabilidades de segurança não detectados na fase de planejamento do projeto.	Baixa	Alto	Contratado	Avaliar o ambiente do projeto em busca de possíveis problemas de segurança.
Sobrecarga de trabalho da equipe	Equipe responsável pela execução do projeto sobrecarregada.	Alta	Médio	Contratado	Reavaliar a distribuição das tarefas do projeto e se necessário adicionar mais recursos para a conclusão do projeto.
Falência ou Concordata do Fornecedor	O fornecedor entra em dificuldades financeiras, impactando a entrega do projeto.	Baixa	Alto	Contratado	Avaliação financeira prévia, cláusulas contratuais de substituição e plano de contingência, bem como ressarcimento a eventuais prejuízos.
Evasão de Profissionais do Contratado	Alta rotatividade ou saída repentina de profissionais essenciais do projeto.	Média	Alto	Contratado	Contratos com cláusulas de continuidade, banco de talentos e plano de sucessão estruturado. Reposição imediata do profissional.

SCGÁS COMPANHIA DE GÁS DE SANTA CATARINA	GETIN - Gerência de Tecnologia da Informação
	Memorial Descritivo
	Soluções de Controle de Acesso e Autenticação Centralizada

Resumo: **Contratação de Soluções de Controle de Acesso e Autenticação Centralizada com suporte por um período de 60 (sessenta) meses.**

7. CONDIÇÕES GERAIS:

7.1 O CONTRATADO deverá iniciar o projeto de implantação das Soluções de Controle de Acesso e Autenticação Centralizada em até 15 (quinze) dias após a assinatura do contrato, e concluir a migração em até 3 (três) meses.
7.2 O CONTRATADO deverá entregar na reunião de kick off o cronograma detalhado das atividades do projeto. Esse cronograma será analisado e deverá ser aprovado pela equipe de TI da SCGÁS para dar início ao projeto.
7.3 O CONTRATADO deverá entregar os serviços de implantação das **Soluções de Controle de Acesso e Autenticação Centralizada** de forma remota e na localidade abaixo de forma presencial se necessário:

Localidade	Endereço
SEDE	Rua Antônio Luz, 255 - Centro Empresarial Hoepcke - Bairro Centro - Florianópolis - SC CEP 88010-410

7.4 O CONTRATADO deverá disponibilizar a documentação técnica do projeto implementado. Essa documentação, deverá ser validada pela equipe de TI da SCGÁS.
7.5 O CONTRATADO deverá garantir o funcionamento das **Soluções de Controle de Acesso e Autenticação Centralizada** ao término do serviço de implantação das soluções ofertadas.
7.6 O CONTRATADO deverá após a implantação das **Soluções de Controle de Acesso e Autenticação Centralizada**, fornecer um treinamento para os Analistas de TI da SCGÁS, apresentando o que foi realizado como também, as informações necessárias para a administração e gerenciamento das soluções ofertadas. O treinamento deverá ter pelo menos uma carga horária mínima de 4 (quatro) horas e deverá ser fornecido de forma presencial na SEDE da SCGÁS.
7.7 O pagamento referente a implantação das **Soluções de Controle de Acesso e Autenticação Centralizada**, será realizado após validação da equipe de TI da SCGÁS e de acordo com o cronograma de pagamento da SCGÁS.
7.8 Para a validação que será realizada pela equipe de TI da SCGÁS informada no item 7.7, serão analisadas o funcionamento das seguintes funcionalidades:

- Identificação de forma transparente dos usuários na rede.
- Validar a Autenticação segura de dois fatores.
- Gerenciamento de convidados para segurança da rede cabeada e wireless.
- Reconhecimento e autenticação dos dispositivos de rede.
- Configuração e funcionamento dos dispositivos que farão Mac-Address By-pass.

SCGÁS COMPANHIA DE GÁS DE SANTA CATARINA	GETIN - Gerência de Tecnologia da Informação
	Memorial Descritivo
	Soluções de Controle de Acesso e Autenticação Centralizada

Resumo: **Contratação de Soluções de Controle de Acesso e Autenticação Centralizada com suporte por um período de 60 (sessenta) meses.**

- Reconhecimento e autenticação dos notebooks, desktops e dispositivos móveis na rede.
- Autenticação nas redes Wireless e Cabeadas na Sede e Bases Operacionais.
- Funcionamento do Portal para visitantes.
- Demais funcionalidades utilizadas no ambiente atual relacionado ao Controle de Acesso e autenticação na rede

7.9 As despesas de deslocamento (passagens, táxi, traslados, pedágios, estacionamentos, etc.), estadia e alimentação, nos casos de atividade nas dependências da SCGÁS, ficam sob responsabilidade do CONTRATADO.
7.10 Serão responsabilidade integral do CONTRATADO todos os serviços a serem realizados em horário não comercial, eventuais acréscimos sobre o valor-hora normal de seus profissionais, atividades realizadas em Sábados, Domingos e Feriados, etc.

ALISON LUIZ MARTINS SCHVEITZER:91992362904

Assinado de forma digital por ALISON LUIZ MARTINS SCHVEITZER:91992362904
DN: c=BR, o=ICP-Brasil, ou=Certificado Digital PF A3, ou=Videoconferencia, ou=27637943000186, ou=AC SyngularID Multipla, cn=ALISON LUIZ MARTINS SCHVEITZER:91992362904
Dados: 2025.03.24 13:13:16 -03'00'

Alison Luiz Martins Schveitzer
Analista de Tecnologia da Informação