GERED/COSEI

CÓDIGO	TÍTULO	VIGÊNCIA	VERSÃO
NORMA 001/2021	NORMA DE ACESSO REMOTO	04/08/2022	2

1 PREFÁCIO

A presente Norma está de acordo com as diretrizes da Política de Segurança da Informação e Comunicação do CIASC para Acesso Remoto.

2 OBJETIVO

O objetivo deste documento é normatizar o acesso remoto aos sistemas e demais recursos computacionais no âmbito da rede corporativa do CIASC e aquelas providas para clientes que optaram por manter a administração por esta empresa. Para tal, objetivamos reduzir os riscos associados às tecnologias empresariais utilizadas para teletrabalho e/ou acesso remoto a recursos computacionais em ambiente de rede local, tais como servidores de acesso remoto e dispositivos de clientes em teletrabalho, de prestadores de serviços terceirizados e de parceiro de negócios. O documento enfatiza a importância de proteger as informações confidenciais transmitidas através de acesso remoto originados de redes externas.

3 ESCOPO

Esta norma se aplica a todos os usuários (clientes, prestadores de serviços, estagiários, empregados, etc.) que utilizam o ambiente do CIASC para acesso a serviços internos na Rede de Governo.

4 TERMOS E DEFINIÇÕES

Para efeito desta Norma aplicam-se os seguintes conceitos e definições:

Segurança da Informação e Comunicação (SIC) – proteção da informação contra ameaças para garantir a continuidade das atividades finalísticas e meio da instituição, minimizar os riscos e maximizar a eficiência e a efetividade das ações realizadas no CIASC.

Incidente em Segurança da Informação – qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações da instituição ou ameaçar a segurança da informação.

Usuário – qualquer pessoa (empregados, clientes, visitantes, estagiários, empregados temporários, prestadores de serviços, colaboradores...) que possua ou não ligação com o CIASC, e que necessite de acesso a um sistema ou recurso computacional do CIASC.

Usuário institucional – usuário que, consideradas as atividades finalísticas e administrativas da CIASC, necessita de acesso a serviços de TIC institucionais e que possui vínculo formal vigente ao CIASC, temporário ou permanente (administradores, membros de órgãos estatutários, empregados, estagiários, bolsistas, menores/jovens aprendizes).

Usuário terceirizado – usuário que é empregado temporário ou terceirizado, que possui um vínculo específico com o CIASC decorrente de contrato.

Usuário externo – usuário que não contempla os requisitos de “Usuário institucional” eque, consideradas as atividades finalísticas e administrativas do CIASC, necessita de acesso a serviços de TIC institucionais de forma temporária (participantes de eventos, colaboradores ou prestadores de serviço cuja forma de relação temporária com a instituição preveja a necessidade de acesso por tempo limitado a um ou mais serviços de TIC institucionais).

Gestor – no caso de usuários institucionais, o gestor é o gerente da área; no caso de usuários terceirizados, é o gestor do contrato; no caso de usuários externos prestadores de serviço a clientes, o gestor o cliente.

VPN – a sigla VPN vem do inglês *Virtual Private Network*, que em tradução livre significa Rede Virtual Privada. Ela utiliza a *internet* para se conectar a uma determinada localidade e assim poder usar seus serviços.

VPN *Site-to-Site* – desta forma, esta conexão segura é disponibilizada para redes inteiras, sem que seja necessário que cada usuário ou dispositivo possua um VPN *Client-to-Site* configurado, individualmente, para trafegar entre as redes.

VPN *Client-to-Site* – é caracterizada por conexões pontuais de usuários remotos à rede, diferentemente de VPNs *Site-to-Site* que tratam de conexões remotas entre redes inteiras.

ZTNA – *Zero Trust Network Access*, fornece um mecanismo de acesso altamente detalhado com base na identidade e comportamento de um usuário.

5 PAPÉIS E RESPONSABILIDADES

5.1 Usuário

- Manter sigilo das informações de acesso ao ambiente de rede do CIASC e da conexão remota, sendo de sua total e exclusiva responsabilidade qualquer operação realizada por meio de suas credenciais de acesso;
- Comunicar imediatamente à área de Segurança da Informação (COSEI) qualquer situação que coloque em risco o acesso ao ambiente da rede de dados do CIASC; e
- Informar seu gestor quando forem identificados direitos de acesso remoto desnecessários à execução dessas atividades.

5.2 Gestor

- Solicitar e/ou revogar as credenciais de acesso remoto dos usuários institucionais ou terceirizados sob sua gestão, incluindo aqueles que estão trabalhando junto com as equipes do CIASC;
- Conscientizar os usuários em seu domínio administrativo quanto às orientações presentes neste documento e nas boas práticas de segurança;
- Comunicar imediatamente ao setor de Segurança da Informação (COSEI) caso verifique qualquer ameaça, vulnerabilidade ou situação que possa colocar em risco o ambiente computacional em questão; e
- Manter atualizada relação de usuários e seus papéis para que, de forma contínua, seja verificada a política de acessos mínimos e com isso a adequação dos perfis de acesso dos respectivos usuários.

5.3 Gerência de *Data Center* (GEDAT)

- Manter a disponibilidade, integridade e confidencialidade do sistema de autenticação de usuários (LDAP).

5.4 Gerência de Redes (GERED)

- Administrar os acessos remotos ao ambiente de rede de dados do CIASC, para acessos pela modalidade “site-to-site” e “c” em *firewall* apropriado para este acesso;
- Manter a disponibilidade, integridade e confidencialidade em todo o ambiente computacional que suporta a solução de acesso remoto “site-to-site” e “client-to-site”;
- Monitorar todo o ambiente de modo a identificar proativamente anomalias e acessos maliciosos;
- Manter os registros de acesso para fins de auditoria respeitando a legislação e as boas práticas de mercado;

- Manter mecanismos de segregação de acesso lógico entre os ambientes de acesso remoto e os recursos computacionais em ambiente de rede local controlando o acesso por meio de políticas de acessos mínimos;
- Manter registro histórico de solicitações de criação e revogação de usuários para fins de auditoria e controle; e
- Efetuar auditorias no ambiente como forma de garantir que os mecanismos de segurança adotados se mantêm eficientes.

5.5 Gerência de Recursos Humanos (GEREH)

- Notificar à equipe da COSEI a criação de credenciais de acesso remoto de empregados admitidos;
- Notificar à equipe da COSEI a revogação de credenciais de acesso remoto de empregados que entrarem em licenças sem vencimento, desligamento definitivo, desligamento temporário por decisão judicial, afastamentos por licença de saúde ou que forem colocados à disposição de outros órgãos onde o prazo de afastamento for superior a um mês;
- Conscientizar os novos empregados quanto às orientações presentes neste documento e nas boas práticas de segurança.

6 DIRETRIZES

6.1 O acesso remoto para pessoa jurídica é de uso exclusivo para parceiros ou prestadores de serviços que necessitem de acesso à rede de Governo mediante cadastro de pessoa física a qual será a responsável legal pela gestão do acesso e cumprimento das normas de segurança da instituição.

6.2 As solicitações de criação de conta de acesso remoto de terceiros contratados para serviços prestados diretamente ao CIASC devem ser feitas ao Gestor, que deverá providenciar a solicitação formal à COSEI.

6.3 As solicitações de criação de conta de acesso remoto de terceiros com a finalidade de prestação de serviço a clientes, ou seja, de usuários que não possuem vínculo contratual com o CIASC, devem ser realizadas através da Gerência de Comercialização (GECOM) do CIASC e serão disponibilizadas segundo os critérios comerciais estabelecidos por esta área e critérios técnicos definidos pela COSEI.

- A solicitação deverá ser formalizada através de formulário específico, com justificativa, serviços e/ou redes a serem acessadas e período de trabalho.
- O perfil de acesso sempre deverá obedecer ao princípio de acessos mínimos de acordo com a real necessidade e justificativa do acesso.
- Estas solicitações devem ser autorizadas pelo gestor da área ou superior imediato e arquivadas para fins de auditoria.

6.4 O acesso remoto de uma rede externa ao ambiente CIASC e/ou o acesso a **serviços internos** na Rede de Governo deverão ser rigorosamente controlados e autorizados, e utilizar criptografia pelo serviço de VPN corporativo provido de autenticação com senha forte.

6.5 O usuário com acesso remoto é autorizado a acessar apenas os serviços e/ou redes que foram justificados, por isso deverá ser associado a perfil que permita que tais limites de acesso sejam implementados.

6.6 Os usuários autorizados ao acesso remoto devem proteger suas credenciais e em nenhum momento devem disponibilizar seu login e senha de rede, *e-mail*, VPN, ou qualquer informação de acesso, para outra pessoa.

- Devem manter sua senha com complexidade alta para aumentar a segurança em sua autenticação. Por exemplo, no mínimo uma letra maiúscula, uma letra minúscula, um número, um caractere especial e 8 dígitos.
- Não devem utilizar a mesma senha que já utilizam em outros serviços de qualquer natureza.

- Devem comunicar imediatamente qualquer anomalia e/ou incidente percebido com seu serviço.

6.7 Os usuários com acesso remoto autorizado devem garantir a não utilização do seu perfil de acesso remoto por outras pessoas, bem como não fazer uso do recurso de VPN em redes não confiáveis e/ou públicas, ou em computadores compartilhados e/ou que não sejam de sua responsabilidade administrativa, para que sejam mitigados riscos de roubo de credenciais, interceptação de tráfego e outras ameaças digitais.

6.8 O usuário, quando da utilização do acesso remoto, deverá permanecer conectado ao servidor de VPN enquanto estiver efetivamente usando os serviços disponibilizados a trabalho, devendo desconectar-se no término das atividades.

6.9 Os usuários com acesso remoto devem cuidar para que informações sigilosas não sejam capturadas por terceiros que estejam próximos ao equipamento.

6.10 Os administradores das soluções de autenticação utilizadas pelas VPNs “client-to-site” e “site-to-site” devem configurar os sistemas de autenticação de modo a não permitir que os usuários consigam efetivar o cadastro de senhas fracas.

6.11 Aos usuários com perfis mais abrangentes de acesso, tais como, administradores de sistemas, administradores de rede, desenvolvedores e administradores de bases de dados, deve ser exigido um segundo fator de autenticação nas conexões de VPN.

6.12 A solução oficial de VPN para acesso remoto de usuários adotada pelo CIASC, na modalidade de “client-to-site”, é composta da seguinte forma:

- FortiClient sem ZTNA para dispositivos particulares.
- FortiClient com ZTNA para dispositivos corporativos.
- OpenVPN para clientes e *disaster recover*.

6.13 Para prestação de suporte remoto a estações de trabalho é permitido o uso de *Google Remote Desktop* utilizando as credenciais oficiais do CIASC (usuario@ciasc.sc.gov.br).

6.14 É vedado o uso de quaisquer outras soluções de acesso remoto diferente das adotadas oficialmente pelo CIASC, tais como o *TeamViewer*, *AnyDesk* e similares sem que haja a autorização expressa da área de Segurança da Informação (COSEI).

7 SANÇÕES

A violação desta política por qualquer usuário será reportada ao CGSI - Comitê Gestor de Segurança da Informação do CIASC e ao superior imediato que liberou o acesso e que poderá tomar medidas para suspender de forma imediata, temporária ou permanente os seus privilégios de acesso à rede local de dados, bem como encaminhar os fatos às áreas pertinentes para aplicação das medidas administrativas cabíveis com vistas a impor as sanções aplicáveis, seja no âmbito de responsabilização interna, através de sanções disciplinares, seja no âmbito externo, às pessoas físicas ou jurídicas, tais como multas e demais sanções previstas em contratos, respeitado o princípio da proporcionalidade e do devido processo legal, sem prejuízo de eventual ação judicial para reparação dos danos e preservação dos direitos desta empresa.

8 REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO/IEC 27002:2013 - Tecnologia da Informação - Técnicas de segurança - Código de prática para a Gestão da Segurança da Informação. Rio de Janeiro: ABNT, 2013.

9 HISTÓRICO DE VERSÕES

Alterações	Data de aprovação	Versão gerada
1ª Versão (inicial)	06/01/2021	1
Versão revisada com adição do suporte remoto pelo *Chrome Desktop* e outras alterações.	04/08/2022	2