POLÍTICA DE SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (PSTIC)

DO CONSELHO REGIONAL DE PSICOLOGIA DA 6ª REGIÃO

2ª EDIÇÃO
SÃO PAULO
2024

Conselho Regional de ***PSICOLOGIA*** *SP*

XVII PLENÁRIO: 2022–2025

Diretoria
Presidenta: Talita Fabiano de Carvalho
Vice-presidenta: Camila Andrade de Oliveira
Secretária: Marta Eliane de Lima
Tesoureiro: Eduardo de Menezes Pedroso

Conselheiras/os efetivas/os:
Ana Tereza da Silva Marques (CRP 06/141032)
Carlos Eduardo Mendes (CRP 06/153775)
Davi Rodriguez Ruivo Fernandes (CRP 06/118838)
Dreyf de Assis Gonçalves (CRP 06/55379)
Ione Aparecida Xavier (CRP 06/27445)
Janaina Darli Duarte Simão (CRP 06/47523)
Magna Barboza Damasceno (CRP 06/66384)
Maria da Piedade Romeiro de Araujo Melo (CRP 06/45952)
Maria da Glória Calado (CRP 06/33194)
Mayara Aparecida Bonora Freire (CRP 06/120511)
Mônica Cintrão França Ribeiro (CRP 06/20583)

Conselheiras/os suplentes:
Gabriela Alvim de Oliveira Freitas (CRP 06/149012)
Giseli de Fátima Assoni (CRP 06/72980)
Leonardo Maggi Gambatto (CRP 06/124424)
Wilson Flávio Lourenço Nogueira (CRP 06/53258)

Renúncias
Annie Louise Saboya Prado (CRP 06/86192)
Carú de Paula Seabra Moreira Ribeiro (CRP 06/136173)
Fabiana Macena Luiz (CRP 06/148611)
Ivani Teixeira Mendes (CRP 06/42535)
Lilian Suzuki (CRP 06/27810)
Murilo Centrone Ferreira (CRP 06/142583)
Sonia Maria Motinho da Silva (CRP 06/12033)
Tayná Alencar Berti de Souza (CRP 06/83455)
Valeria Campinas Braunstein (CRP 06/31093)

Vacâncias
Camila Prandini Prandini (CRP 06/157432)
Luciane de Almeida Jabur (CRP 06/66501)

PROJETO GRÁFICO
Micael Melchiades

REVISÃO TEXTUAL
Angelo Cuissi

APRESENTAÇÃO DA 2ª EDIÇÃO

Passados dez meses de implantação da atual Política de Segurança em Tecnologia da Informação e Comunicação (PSTIC), novos recursos e fluxos tecnológicos foram implantados, tornando necessária sua atualização.

O desafio de instituir uma política institucional dentro de uma autarquia pública federal que, durante muitos anos, atuou em processos diversos e difusos sem padronização e formalidade, coloca-nos em situação de maior atenção e responsabilidade.

Identificamos resistências e dúvidas quanto aos procedimentos institucionais e maior necessidade de elucidação das ações.

O desafio de garantir a governança preconizada para a administração pública envolve três funções básicas, alinhadas às tarefas sugeridas pela ISO/IEC 38500:2008:

a. avaliar o ambiente, os cenários, o desempenho e os resultados atuais e futuros;
b. direcionar e orientar a preparação, a articulação e a coordenação de políticas e planos, alinhando as funções organizacionais às necessidades das partes interessadas (usuária/os dos serviços, cidadãos e sociedade em geral) e assegurando o alcance dos objetivos estabelecidos;
c. monitorar os resultados, o desempenho e o cumprimento de políticas e planos, confrontando-os com as metas estabelecidas e as expectativas das partes interessadas.

O Acórdão 1768/2022 do TCU visa contribuir para a transformação digital do país, conscientizando os gestores públicos acerca dos riscos aos quais as organizações estão sujeitas, de modo que sejam implementados controles e medidas de segurança adequados para enfrentá-los.

Assim, o TCU estabelece os "Cinco controles de segurança cibernética para ontem" para embasar a adoção, pelas organizações públicas federais, dos controles críticos de cibersegurança que se seguem:

Controle 1 — Inventário e controle de ativos corporativos: identificar e impedir a utilização de ativos de TI não autorizados/gerenciados como vetores de ataques cibernéticos;
Controle 2 — Inventário e controle de ativos de *software:* identificar e impedir a utilização de *softwares* não autorizados/gerenciados como vetores de ataques cibernéticos;
Controle 7 — Gestão contínua de vulnerabilidades: evitar a exploração de vulnerabilidades conhecidas nos ativos corporativos de TI;
Controle 14 — Conscientização sobre segurança e treinamento de competências: reduzir a possibilidade de incidentes e ataques derivados do comportamento humano (engenharia social);

Controle 17 — Gestão de respostas a incidentes: melhorar a capacidade de identificar potenciais ameaças e ataques, evitar que se espalhem e recuperar rapidamente dados e sistemas eventualmente corrompidos.

Também a publicação da Portaria CRP-06 nº 99/2024, que "estabelece a jornada de trabalho de 30 horas semanais e o teletrabalho no âmbito do Conselho Regional de Psicologia da 6ª Região, cria e regulamenta o regime híbrido de trabalho e dá outras providências" nos coloca a necessidade de regulamentar com mais rigor o uso das tecnologias da informação e comunicação.

Esta nova edição apresenta inovações em diferentes âmbitos, seja pela inserção de tutoriais de acesso aos sistemas e programas, seja pela atualização de ferramentas para abertura de chamados e reformulação de fluxos;

...propõe uma ponte com o Código de Ética da Sociedade Brasileira de Computação, um avanço na vinculação prática do compromisso ético de nossa profissão aos princípios ali indicados para a oferta de serviços de qualidade a sociedades;

...incorpora normativas convergentes na defesa intransigente da democracia e da Psicologia: a Lei de Acesso à Informação (LAI; Lei nº 12.527/2011), o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (LGPD; Lei nº 13.709/2018), fundamentando, assim a expressão prática do espírito destas.

Assim, apresentamos a segunda edição da presente Política com o foco no aprimoramento, na qualificação e na inovação dos fluxos e procedimentos institucionais.

Talita Fabiano de Carvalho
Conselheira presidenta do CRP-06

APRESENTAÇÃO DA 1ª EDIÇÃO

O Conselho Regional de Psicologia de São Paulo — 6ª Região (CRP SP), entidade dotada de personalidade jurídica de direito público, com autonomia administrativa e financeira, nos termos da Lei Federal nº 5.766, de 20 de dezembro de 1971, tem como finalidade fiscalizar o exercício da profissão de psicóloga/o, competindo-lhe orientar, disciplinar e zelar pela fiel observância dos princípios ético-profissionais e contribuir para o desenvolvimento da Psicologia enquanto ciência e profissão.

Este CRP SP tem sede na cidade de São Paulo e jurisdição no estado de São Paulo, possuindo subsedes nas regiões de Alto Tietê (Mogi das Cruzes), Assis (Assis), Baixada Santista e Vale do Ribeira (Santos), Bauru (Bauru), Campinas (Campinas), Grande ABC (Santo André), Metropolitana (São Paulo), Ribeirão Preto (Ribeirão Preto), São José do Rio Preto (São José do Rio Preto), Sorocaba (Sorocaba) e Vale do Paraíba e Litoral Norte (Taubaté).

O CRP SP tem como atribuições principais: adotar as medidas e procedimentos necessários à permanente orientação, disciplina e fiscalização do exercício da profissão de psicóloga/o no estado de São Paulo; adotar medidas e procedimentos para preservação do livre exercício da profissão de psicóloga/o, bem como do respeito às suas prerrogativas e direitos profissionais; executar os serviços concernentes ao registro profissional das/os psicólogas/os, realizando as inscrições, reativações, transferências e cancelamentos de registros, expedindo às/aos inscritas/os a carteira de identidade profissional (CIP); funcionar como tribunal regional de ética profissional; elaborar e encaminhar ao Conselho Federal de Psicologia (CFP) a proposta orçamentária anual, além do relatório geral de suas atividades; providenciar a instalação da Assembleia Geral das/os psicólogas/os inscritas/os na região; arrecadar anuidades, taxas e demais rendimentos que lhe competem, promovendo o repasse da arrecadação ao Conselho Federal; criar os serviços necessários ao bom desempenho de suas atividades e autorizar a compra de material para suas instalações; organizar o quadro de pessoal; zelar pela dignidade, independência, prerrogativas e valorização da Psicologia; e zelar pela gestão responsável, cumprindo a legislação a partir dos princípios da administração pública: legalidade, impessoalidade, moralidade, publicidade e eficiência.

Assim, para uma adequada utilização dos recursos e dispositivos públicos, foi aprovado, no Planejamento Estratégico 2023–2025, resultado específico para garantir a implantação adequada dos sistemas e instrumentos oficiais do CRP SP.

O Resultado 1.2 do Planejamento Estratégico supracitado se refere a "ter implementado estrutura de gestão democrática com processos de trabalho planejados e institucionalizados, de forma transversal, acessível, integrada, transparente e com produção de dados."

Das ações previstas para 2023, foi atingido o Resultado 1.2: "Ter implantado e integrado os sistemas informatizados (SEI, BRC, Benner e produtos Zimbra/Implanta), garantindo o cumprimento das normativas (leis, resoluções, Corep), dos fluxos e processos de trabalho com formação permanente, transparência, produção, análise e segurança de dados."

E, por fim, fazendo cumprir a Macroação nº 8 — "Ter elaborado política que institucionaliza e da segurança ao uso dos novos sistemas" —, é elaborada esta Política de Segurança em Tecnologia da Informação e Comunicação (PSTIC), que especifica os controles internos aplicáveis à segurança, ao sigilo da informação e ao uso das ferramentas do Conselho Regional de Psicologia da 6ª Região — CRP SP, com o objetivo de realizar suas operações gerais, ainda que

em situações adversas.

Estão sujeitas/os ao disposto no presente documento todas/os as/os conselheiros, colaboradoras/es, trabalhadoras/es, funcionárias/os terceirizadas/os, estagiárias/os, prestadoras/es de serviços e demais convidadas/os, no que a cada um for aplicável.

A Política Segurança da TIC é o documento que normatiza, orienta e estabelece as diretrizes para a proteção dos sistemas, documentos, operações e comunicação institucional quanto a processos de trabalho e uso da rede e, principalmente com a prevenção de responsabilidade legal para todos as/os usuárias/os.

Além disso estabelecimento de fluxos para comunicação e guarda de documentos e deve, portanto, ser cumprida e aplicada em todas as áreas da autarquia.

A presente política está baseada nas leis vigentes brasileiras que tangem sobre isso, bem como nas recomendações propostas pelas ABNT NBR ISO/IEC 27002/2022, reconhecida mundialmente como um código de prática para a gestão da segurança da informação.

Também é importante destacar que esta política visa apoiar inicialmente a Lei Geral de Proteção dos Dados — LGPD (Lei nº 13.709/2018), segundo a qual toda a informação produzida ou recebida como resultado da atividade institucional pertence ao CRP SP.

Por fim, garantimos aqui que os registros institucionais sejam disponibilizados no Portal da Transparência do CRP SP preconizado pela Lei de Acesso à Informação (Lei nº 12.527/2011) tomadas as devidas proteções ao sigilo daqueles documentos internos que ficarão guardados pela autarquia.

Talita Fabiano de Carvalho
Conselheira presidenta do CRP-06

SUMÁRIO

1 DOS OBJETIVOS E RESPONSABILIDADES

1.1 DOS OBJETIVOS

a) Estabelecer diretrizes que permitam a todas as pessoas usuárias dos sistemas e ferramentas de tecnologia da informação e comunicação (TIC) do CRP–06 seguir padrões de comportamento relacionados à segurança da informação adequados às necessidades institucionais e à proteção legal das/os envolvidas/os;
b) normatizar e orientar todas as pessoas usuárias para a proteção dos sistemas, documentos, operações e comunicação institucional no que tange aos processos de trabalho e uso das redes, principalmente com a prevenção de responsabilidade legal;
c) definir normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.
d) ofertar orientações sobre a utilização dos recursos computacionais, de telecomunicação e de infraestrutura de TI;
e) garantir a integridade da informação para que seja mantida em seu estado original, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;
f) garantir a confidencialidade e que o acesso à informação seja obtido somente por pessoas autorizadas e exclusivamente em função do interesse público;
g) garantir a disponibilidade para que as/os usuárias/os autorizadas/os obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
h) assegurar a aplicabilidade das referências e diretrizes da governança da informação preconizadas pelo Tribunal de Contas da União (TCU);
i) organizar fluxos institucionais para tramitação de processos, informações, solicitações e respostas;
j) garantir a lisura, transparência e responsabilidade para com os processos institucionais.

1.2 DAS RESPONSABILIDADES

Os recursos institucionais disponíveis na autarquia são de uso exclusivo da e para as atividades e ações institucionais.

a) O CRP-06 não se responsabiliza pelas perdas causadas pelo uso indevido, negligente ou imprudente dos recursos e/ou serviços concedidos a suas/seus usuárias/os;
b) o CRP-06, por meio da Unidade de Tecnologia da Informação e Comunicação, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas, inclusive revisando e atualizando estas normas sempre que algum fato e/ou evento relevante acontecer;
c) todos os contratos firmados com as/os usuárias/os do CRP-06 deverão ser previamente formalizados via termo de acordo do uso e confidencialidade (TAUC), condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição;
d) qualquer incidente que afete a segurança da informação deverá ser comunicado inicialmente à coordenação de TIC e ela, após análise encaminhará à Gerência Administrativa e de Tecnologia da Informação (GATI) para que as medidas corretivas possam ser tomadas. Se necessário, a Unidade de Gestão de Pessoas e/ou a diretoria poderão ser envolvidas para apoiar a decisão;
e) a fim de garantir maior segurança no uso dos sistemas da autarquia, faz-se necessária a segregação dos ambientes de desenvolvimento (uso da TI), testes (uso da TI e colaboradores-chave para testes), homologação (uso da TI) e produção (uso institucional);
f) o CRP-06 reserva-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis;
g) é vedado o uso de todo e qualquer meio não institucional de contas e dispositivos pessoais como *e-mails* que não sejam institucionais, WhatsApp, Skype, redes sociais e outros fora do domínio da rede formal;
h) é importante destacar que nenhuma pessoa deve ser lesada no uso de seus recursos pessoais, pois a autarquia oferece ferramentas necessárias para a comunicação institucional;
i) qualquer outro instrumento institucional (*e-mail, chat*, aplicativo de mensagem instantânea, entre outros) não possui a prerrogativa deliberativa nem substitui, sob qualquer hipótese, aqueles já previstos, como ofício, memorando, despacho, portaria, instrução normativa ou resolução;
j) nas situações de não cumprimento, parcial ou integral, por parte da/o usuária/o, dos requisitos previstos nesta Política e das orientações sobre a segurança da informação, bem como das regras internas da autarquia, a/o usuária/o será submetida/o às medidas administrativas e legais cabíveis;
k) o uso pessoal dos recursos institucionais em hipótese alguma possui caráter deliberativo ou legal e é expressamente vedado e, caso ocorra, resultará na aplicação de medidas previstas na legislação pertinente para apuração dos fatos e responsabilização das/os envolvidas/os;
l) será de inteira responsabilidade de cada usuária/o o prejuízo ou dano que vier a sofrer ou causar ao CRP-06 e/ou a terceiros, em decorrência do não cumprimento às diretrizes e normas aqui referidas.

1.2.1 Das responsabilidades específicas

1.2.1.1 Das/os conselheiras/os, gestoras/es, funcionárias/os, colaboradoras/es, terceirizadas/os, estagiárias/os, prestadoras/es de serviços e demais convidadas/os

a) Zelar pelo cumprimento desta Política, de forma a garantir a segurança da informação e assegurar o uso adequado dos meios, realizando *backups* periódicos dentro da infraestrutura disponível, não compartilhando senhas e não disseminando notícias ou informações inconsistentes, sigilosas ou institucionais fora dos instrumentos da autarquia;
b) exigir das/os usuárias/os sob sua responsabilidade o devido cumprimento desta Política;
c) exigir e condicionar o uso à assinatura do termo de uso e confidencialidade e o seguimento das normas estabelecidas, bem como ao compromisso de manter sigilo e confidencialidade sobre todos os ativos de informações do CRP-06, elucidando dúvidas e encaminhando para suporte as dificuldades técnicas, quando necessário.

1.2.1.2 Da Unidade Administrativa de Tecnologia da Informação

a) Informar às/aos gestores os serviços específicos que serão prestados e os procedimentos de resposta aos incidentes, atualizando, assim, o manual de serviços sempre que necessário;
b) configurar os equipamentos, ferramentas e sistemas concedidos às/os usuárias/os com todos os controles necessários para cumprir e assegurar os requisitos de segurança e uso estabelecidos por esta Política;
c) permitir, quando necessária, a execução de atividades operacionais sob sua responsabilidade, como, por exemplo, manutenção de computadores, realização de cópias de segurança, criação de contas para acesso institucional ou testes no ambiente;
d) seguir as normas e/ou orientações do Sistema Conselhos de Psicologia e da legislação vigente, no que diz respeito à segurança da informação para todos os Sistemas e aplicações com acesso público;
e) planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessária para garantir a segurança requerida pelas áreas de atuação, fundamentando tecnicamente seus procedimentos e encaminhamentos;
f) atribuir cada conta ou dispositivo de acesso (computadores, celulares, *tablets* e outros), dispositivos dos sistemas, bases de dados ou qualquer outro ativo de informação a uma/um responsável identificável como pessoa física, de acordo com a Lei Geral de Proteção de Dados (LGPD);
g) proteger continuamente todos os ativos de informação do CRP-06 contra código malicioso, garantindo que os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado e após auditados por esta unidade administrativa;
h) propor a definição de regras formais para instalação de *software e hardware* em ambiente de produção institucional, implementando as diretrizes do Código de ética da Sociedade Brasileira de Computação em consonância com o Código de Ética Profissional da/o Psicóloga/o;
i) realizar manutenções corretiva, evolutiva e preventiva mensalmente, a fim

de revisar tecnicamente os dispositivos tecnológicos de trabalho e mitigar possíveis riscos para assegurar o bom funcionamento dos recursos, a partir de plano de trabalho e cronograma devidamente aprovados pelo plenário;

j) auxiliar na instalação e configuração de assinaturas digitais e certificados digitais, por meio de ferramentas específicas;

k) promover os meios e estabelecer as diretrizes de orientação para as/os usuárias/os quanto à política de *backup* de dados, e auditá-los quando necessário;

l) garantir, de maneira rápida e eficaz, após solicitação formal, o bloqueio de acesso de usuária/o por motivo de desligamento, incidente, investigação ou outra situação que exija medida restritiva para fins de resguardo dos ativos do CRP - 06;

m) dar suporte operacional atitudinal na implementação, manutenção e promoção da cultura e desenvolvimento das ações e processos para uso de todos os sistemas, redes e ativos da autarquia, com base nos princípios éticos da área, de modo coerente com esta política.

1.2.1.2.1 Da responsabilidade de garantia da segurança de informação e comunicação

a) Publicar e promover as edições necessárias desta Política de Segurança em Tecnologia da Informação e Comunicação, com base em princípios técnicos;

b) promover a conscientização das/os usuárias/os em relação à relevância da segurança da informação, mediante campanhas e informativos, gestão de termos de cessão de uso e responsabilização;

c) analisar criticamente incidentes recorrentes e outros problemas em conjunto com usuária/o, fornecedores e, no caso dos Sistemas Federais, junto ao Comitê de TI do Conselho Federal de Psicologia;

d) analisar técnica e criticamente incidentes recorrentes e outros problemas de fornecedoras/es prestadoras/es de serviços em conjunto com as gerências e coordenações de cada unidade, elaborar parecer técnico fundamentado para dar subsídio à gerência de competência e dar ciência ao plenário, efetuando a gestão de contratos de uso e prestação de serviços;

e) exercer a continua práxis de alinhamento com as diretrizes institucionais da autarquia e normas regulamentadoras de segurança da informação e comunicação a partir de leis e normativas dos órgãos de controle.

2 DA GRAVAÇÃO DAS REUNIÕES

Todas as reuniões do CRP SP devem ser gravadas para fins de registro posterior, não sendo permitido o compartilhamento das gravações com terceiros ou com as partes sem autorização expressa de todos os participantes.

Quanto à proteção dessas gravações, fica determinado que:

a) somente a Unidade de Secretaria terá acesso às gravações para registro das reuniões, sendo obrigatória a exclusão do arquivo após a aprovação do documento;
b) em caso de ata ou registro aprovado ao final da própria reunião, a gravação deve ser imediatamente excluída;
c) em casos de gravação para fins de treinamento, capacitação e demais ações pedagógicas, todas/os as/os participantes devem autorizar expressamente sua divulgação no início da atividade, em conjunto com o registro da finalidade e da limitação de tal compartilhamento;
d) os assuntos discutidos nas reuniões ordinárias, extraordinárias, assembleias ou similares e os registros de suas informações são passíveis de divulgação e de acesso, com exceção das partes que expressamente tiverem sigilo previsto em hipóteses legais e/ou possam violar os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD; Lei nº 13.709/2018).

3 DO MONITORAMENTO E DA AUDITORIA

Para promover a proteção, é necessário que haja processos básicos, porém definidos e aplicáveis, delineados em uma estratégia de segurança eficaz que contemple os três fatores bem estruturados — pessoas, processos e tecnologias —, para que se realize a jornada completa de segurança da autarquia, mitigando os riscos a que está exposta.

Esses processos visam garantir a integridade, a confidencialidade e a disponibilidade de dados armazenados e evitar prejuízos. Implementá-los, bem como zelar pelo rigoroso cumprimento das diretrizes e fluxos aqui definidos, são algumas das funções da auditoria de segurança da informação.

A auditoria, portanto, é uma avaliação sistemática e abrangente dos sistemas de segurança da informação, permitindo sua avaliação e também a dos processos e políticas de segurança. Seu objetivo principal é identificar possíveis vulnerabilidades e brechas de segurança para que medidas de proteção adequadas possam ser implementadas com a frequência cabível.

Esta Política determina dois tipos de auditoria de segurança da informação: a interna e a externa.

A auditoria interna, feita pelo Grupo Gestor da TI, é responsável por verificar e analisar os sistemas e procedimentos internos da instituição.

A auditoria externa pode ser feita por uma empresa terceirizada e que não tenha vínculo com a contratante, podendo ser contratada sempre que necessário.

Essa auditoria visa atingir:

a) garantia de ética e conformidade dos sistemas e dispositivos institucionais;
b) conformidade com as leis e regulamentações de proteção de dados;
c) prevenção de invasões e corrompimento de dados;
d) segurança do ambiente de trabalho e confiabilidade;
e) garantia de melhor desempenho e produtividade com os dispositivos institucionais;
f) identificação de riscos de segurança e das vulnerabilidades dos sistemas;
g) prevenção de futuros problemas;
h) identificação de áreas que precisam de atenção e processos mais vulneráveis;
i) prevenção de perdas financeiras, uso inadequado dos recursos, proteção da reputação da autarquia e vazamentos de dados;
j) preparação para lidar com ameaças de segurança e recuperar as capacidades em caso de falha no sistema ou vazamento de dados.

Assim, realizar auditorias regulares pode ajudar a identificar pontos fracos na infraestrutura de TI, verificar os controles de segurança e monitorar o cumprimento destas diretrizes.

Por fim, fica instituída a realização, a qualquer tempo, de inspeção física ou lógica nos recursos tecnológicos de sua corresponsabilidade, em caráter de manutenção preventiva, corretiva ou evolutiva, além da instalação de sistemas de proteção, preventivos e detectáveis, sempre que possível.

3.1 ETAPAS

3.1.1 Planejamento

Deverá ser definido anualmente o escopo da auditoria, identificando-se áreas críticas que precisem ser avaliadas e designando-se uma equipe responsável pela auditoria. Deverão, também, ser estabelecidos objetivos e metas para a auditoria e um cronograma para sua execução.

3.1.2 Coleta de informações

Coletar informações sobre a autarquia, sistemas e processos, o que pode incluir entrevistas com funcionários, revisão de documentos e análise de sistemas e infraestrutura.

3.1.3 Análise de riscos

Com base nas informações coletadas, deve-se realizar uma análise de risco para identificar as principais ameaças e vulnerabilidades da organização.

3.1.4 Avaliação de controles

Avaliar os controles de segurança existentes na organização, como políticas, procedimentos e tecnologias de segurança.

3.1.5 Relatórios e recomendações

Preparar um relatório detalhado com principais descobertas e recomendações para mitigar os riscos identificados.

3.1.6 Acompanhamento

Realizar um acompanhamento para garantir que as recomendações foram implementadas corretamente e que os riscos foram mitigados.

4 DA UNIDADE ADMINISTRATIVA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (TIC) DO CRP-06

4.1 DO GRUPO GESTOR DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Visa coordenar e acompanhar as ações de Tecnologia da Informação e Comunicação do CRP-06, bem como propor estratégias para o melhor uso dos sistemas, dispositivos e fluxos da autarquia na gestão da informação e comunicação.

Deve ser composto no mínimo por:

a) diretoria;
b) Comissão de Auditoria e Controle Interno — Caci;
c) gerências;
d) coordenação da Unidade Administrativa de Tecnologia da Informação.

4.2. DA UNIDADE ADMINISTRATIVA DE TECNOLOGIA DA INFORMAÇÃO

Composta pelas/os trabalhadoras/es efetivas/os da Unidade Administrativa da Tecnologia da Informação do CRP-06 (Resolução CRP-06 nº 03/2022), visa otimizar e facilitar o atendimento das/dos usuárias/os, bem como melhorar a qualidade do serviço prestado por intermédio de formulação e acompanhamento de indicadores, primando pelo uso de dados abertos e legíveis por máquina.

4.2.1 Contatos para suporte

E-mail	Descrição do suporte	Horário	Responsável
informatica@crpsp.org.br	internet/telefonia hardware rede/monitoramento segurança NextCloud Zimbra SEI!	9h às 18h	André Caio Carlos
sistemas@crpsp.org.br	BRC BRC (serviços *on-line*)	9h às 18h	Wellington Denise Carlos
carlos.vasconcelos@crpsp.org.br	Novos projetos	10h às 19h	Carlos

4.2.1.1 Suporte à rede (internet e wi-fi), monitoração de segurança, equipamentos e serviços Zimbra e Nextcloud

O suporte à rede, monitoração de segurança, equipamentos, serviços Zimbra, Nextcloud e SEI! será prestado pela equipe de Tecnologia da Informação, de segunda a sexta-feira, das 9h às 18h.
Chamados deverão ser direcionados para o *e-mail*: informatica@crpsp.org.br.

4.2.1.2 Suporte ao SEI!

O suporte ao SEI! será prestado pelo trabalhador Caio, de segunda a sexta-feira, das 9h às 18h.
Chamados deverão ser direcionados para o *e-mail*: informatica@crpsp.org.br.

4.2.1.3 Suporte aos sistemas BR Conselhos e BRC Serviços Online

O suporte aos serviços ligados ao BRC será prestado pelo trabalhador Wellington, de segunda a sexta-feira, das 9h às 18h.
Chamados deverão ser direcionados para o *e-mail*: sistemas@crpsp.org.br.

4.2.1.4 Novos projetos

Todos os novos serviços que forem demandados para a TI que não sejam chamados, conforme descrito nos itens anteriores, e que demandem atividades técnicas e de sistema, serão tratados como novos projetos de TI e deverão obedecer ao seguinte cronograma:

a) a solicitação deverá ser direcionada para o *e-mail* carlos.vasconcelos@crpsp.org.br, com descrição do projeto e o máximo possível de informações, como cronograma esperado, informações quantitativas, etc.;
b) após a abertura do chamado, será organizada uma reunião de *kick off* com todas/os as/os envolvidas/os;
c) a reunião deverá apresentar o escopo do projeto, definir o cronograma, a avaliação de riscos e a matriz de responsabilidades;
d) após a reunião, o projeto será criado no Deck, no sistema de nuvem Nextcloud;
e) Todas/os as/os envolvidas/os terão acesso ao projeto no Deck, que irá gerenciar todas as atividades, responsabilidades, cronograma, comunicação e entrega do projeto.

4.2.1.4.1 Dos resultados esperados

a) Visibilidade das etapas do projeto por todas/os as/os envolvidas/os;
b) escopo, documentos e cronograma controlados por uma única ferramenta;
c) identificação dos incidentes que poderão impactar no projeto;
d) visibilidade dos projetos em andamento, o que permitirá elaborar cronogramas mais consistentes;
e) acompanhamento dos riscos identificados no planejamento, o que irá trazer maior segurança para o andamento do projeto.

5 DAS NORMAS DE CONTROLE DE ACESSO

a) Os *logins* e senhas da conta institucional são pessoais e protegem a identidade da/o usuária/o, e não poderão ser compartilhados com outras pessoas em nenhuma hipótese. Tais dispositivos evitam e previnem que uma pessoa se faça passar por outra perante o CRP-06;
b) não é permitida a criação de contas/listas de transmissão ou de distribuição em nome de coletivos ou unidades administrativas que não possam identificar a pessoa física que receberá ou responderá pessoalmente pela conta;
c) o uso dos *logins* e/ou senhas de outra pessoa constitui infração criminal nos moldes da legislação vigente;
d) a/o usuária/o vinculado a tais dispositivos será responsável pelo seu uso correto perante a autarquia e a legislação;
e) é expressamente proibido o compartilhamento de *login*/senha para funções de administração de sistemas.
f) a Unidade Administrativa de Tecnologia da informação responde pela criação da identidade lógica das/os usuárias/os na instituição.
g) ao realizar o primeiro acesso no ambiente do CRP-06 e no *e-mail* institucional, a/o usuária/o deverá trocar imediatamente a sua senha, conforme as orientações apresentadas;
h) todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários ou em caso de desligamento de qualquer conselheira/o, trabalhadora/trabalhador e/ou colaboradora/colaborador;
i) eventualmente, os dados da/o usuária/o desligada/o poderão ser acessados, somente com a autorização da diretoria, a título de backup das informações;
j) a Unidade de Gestão de Pessoas, a Unidade de Compras e/ou a Unidade de Secretaria deverão imediatamente comunicar o desligamento à Unidade de TI, a fim de que essa providência seja tomada;
l) em caso de esquecimento de sua senha, a/o usuária/o deverá solicitar formalmente uma nova junto à Unidade de TIC.

6 DOS RECURSOS TECNOLÓGICOS (COMPUTADORES, *NOTEBOOKS*, CELULARES, *TABLETS*)

a) Os equipamentos do CRP-06 disponibilizados às/aos usuárias/os devem ser utilizados exclusivamente para as atividades institucionais;

b) é proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação de *hardware* e/ou *software*, sem o conhecimento prévio e o acompanhamento de uma/um técnica/o da TI do CRP-06;

c) as áreas que necessitarem de manutenção deverão solicitá-la previamente por meio da abertura do chamado técnico à TI por *e-mail*;

d) todas as atualizações e correções de segurança do sistema operacional, *softwares* ou aplicativos, somente poderão ser realizadas após a devida validação no respectivo ambiente de homologação, cabendo à equipe de TI a disposição destas atualizações em ambiente de produção;

e) os sistemas e computadores devem ter versões apenas do *software* antivírus institucional instaladas, ativadas e atualizadas. Em caso de suspeita de vírus ou problemas na funcionalidade, a/o usuária/o deverá acionar o departamento técnico responsável mediante registro de chamado;

f) não será responsabilidade do CRP-06 a violação de acessos pessoais e/ou não compatíveis com as atividades desempenhadas pela/o usuária/o, como compras pessoais *on-line*, acesso a *sites* de banco etc.;

g) a transferência e/ou a divulgação de qualquer *software*, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação da/o solicitante, via Unidade de TI;

h) arquivos pessoais e/ou não correspondentes as atividades institucionais — fotos pessoais, músicas e vídeos, entre outros — não deverão ser copiados/movidos para os *drives* de rede;

i) caso identificada a existência desses arquivos, eles poderão ser eventualmente excluídos mediante comunicação prévia à/ao usuária/o;

j) os documentos institucionais deverão ser salvos em volumes de rede. De forma suplementar, poderá ser utilizado o serviço Nextcloud da conta institucional da/o usuária/o para realizar cópia das informações previamente disponibilizadas em rede;

    I. tais arquivos, se gravados apenas nos computadores — por exemplo, no *drive* C: ou em outro meio físico ou virtual não validado pela TI — não terão garantia de *backup* e poderão ser perdidos caso ocorra uma falha no computador. Neste caso, a responsabilidade é da/o própria/o usuária/o;

k) as/os usuárias/os de contas privilegiadas (conselheiros e gestores) não devem, sem a prévia solicitação e a autorização da coordenação de TI, executar nenhum tipo de comando ou programa que venha a sobrecarregar os serviços existentes na rede institucional. Em caso de dúvida, a TI deverá ser acionada;

l) no uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser necessariamente atendidas:

    I. A utilização de senha de segurança para acesso os dispositivos;

    II. todos os computadores de uso individual deverão ter senha na BIOS para restringir o acesso de colaboradoras/es não autorizados. Tais senhas serão definidas pela Tecnologia da informação, que terá acesso a estas para manutenção dos equipamentos;

    III. as/os usuárias/os devem informar à Unidade de TI qualquer identificação de dispositivo estranho conectado ao seu computador;

    IV. é vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por uma/um técnica/o

da TI ou por terceiros devidamente contratados para o serviço;

V. uma vez assumida a responsabilidade como usuária/o de informações, a pessoa deverá manter a configuração do equipamento disponibilizado, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da autarquia;

VI. quando não estiverem sendo utilizados, todos os terminais de computador, *notebook* e impressoras deverão ser protegidos por senha;

VII. todos os recursos tecnológicos adquiridos pelo CRP-06 devem ter, imediatamente, suas senhas padrões (*default*) alteradas pela TI;

m) fica proibido o uso de computadores e recursos tecnológicos do CRP-06 para:

I. tentar obter acesso não autorizado a outro computador, servidor ou rede;

II. burlar quaisquer sistemas de segurança;

III. acessar informações confidenciais sem explícita autorização do proprietário;

IV. vigiar secretamente conteúdo indevido por meio de *softwares* analisadores de pacotes;

V. interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

VI. usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, propaganda política, assédio sexual ou moral, perturbação, caos institucional, difamação, truculência, manipulação, ou supressão de direitos autorais ou propriedades intelectuais;

VII. hospedar material de conteúdo pornográfico, racista, machista, capacitista ou que viole a moral, a ordem pública, e ainda, que viole a dignidade humana e as leis nacionais ou tratados internacionais de que o Brasil seja signatário;

VIII. utilizar *software* pirata, atividade considerada delituosa de acordo com a legislação nacional;

IX.transmitir mensagens em massa sem endereçar os interessados no conteúdo.

As infrações terão como encaminhamento as medidas punitivas adotadas previstas.

7 DO CORREIO ELETRÔNICO — *E-MAIL*

a) O uso do correio eletrônico é para fins exclusivamente institucionais relativos à tramitação de informações, e usará o domínio @crpsp.org.br;

b) o *e-mail* deve ser um meio rápido de resposta, e não um sistema de armazenamento de dados, que devem ser armazenados na rede;

c) é proibida a utilização do *e-mail* institucional para deliberações de qualquer natureza, tramitação de documentos confidenciais ou sigilosos e mensagens com fins expositivos, truculentos, caluniosos ou difamatórios contra qualquer pessoa;

   I. listas de distribuição/transmissão somente serão usadas para tramitação de comunicação institucional de memorandos e demais documentos oficiais, exclusivamente de Unidades Administrativas e entre trabalhadoras/es, sendo vedado seu uso para solicitação de informações, para deliberações de qualquer natureza, tramitação de documentos confidenciais ou sigilosos e mensagens com fins expositivos, truculentos, caluniosos ou difamatórios;

d) em caso de desligamento, o serviço será ser bloqueado, cabendo a notificação prévia desta ação à Secretaria/Gestão de Pessoas, que comunicará à TI;

e) cabe à TI realizar a gestão das contas sob domínio institucional, sendo efetuado bloqueio por três meses no caso de não utilização do *e-mail*, licença e/ou desligamento;

   I. os dados deverão ser solicitados pela/o gestora/gestor imediata/o antes do término deste prazo. A não manifestação dentro do prazo pode tornar a informação irrecuperável;

f) é VEDADO o uso do correio eletrônico para:

   I. enviar mensagem em nome e/ou conta de outra/o usuária/o sem a devida autorização;

   II. armazenar documentos institucionais que deveriam constar da rede de computadores;

   III. deliberações de qualquer natureza, tramitação de documentos confidenciais ou sigilosos e mensagens com fins expositivos, truculentos, caluniosos ou difamatórios;

   IV. enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o CRP-06 e suas unidades vulneráveis às ações civis ou criminais;

   V. divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins, sem autorização expressa e formal concedida pela/o proprietária/o desse ativo de informação;

   VI. falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

   VII. produzir, transmitir ou divulgar mensagem que:

      a. contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses públicos do CRP-06.

      b. contenha ameaças eletrônicas, como: *spam*, *mail bombing*, vírus de computador, *phishing*;

      c. contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;

      d. vise obter acesso não autorizado a outro computador, servidor ou rede;

      e. vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

      f. vise burlar qualquer sistema de segurança;

      g. vise vigiar secretamente ou assediar outra/o usuária/o;

      h. vise acessar informações confidenciais sem explícita autorização da/o proprietária/o;

      i. vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

j. inclua imagens criptografadas ou de qualquer forma mascaradas;

k. tenha conteúdo considerado impróprio, obsceno ou ilegal, seja de caráter calunioso, difamatório, truculento, ofensivo, violento, pornográfico, que gere caos institucional, entre outros;

l. contenha perseguição preconceituosa baseada em gênero, raça, incapacidade física ou mental ou outras situações protegidas;

m. tenha fins políticos locais ou nacionais;

n. inclua material protegido por direitos autorais sem a permissão da/o detentora/detentor dos direitos;

VIII. a notificação de infrações e a aplicação de eventuais medidas punitivas caberão às gerências e à diretoria, em conjunto com a equipe de Gestão de Pessoas;

IX. nos casos mais graves, será aberta sindicância para apurar os fatos e tomar as medidas legais cabíveis, sem prejuízo de instauração de processo administrativo disciplinar, caso os fatos sejam evidentes e não necessitem de apuração prévia;

X. as mensagens de correio eletrônico deverão obrigatoriamente incluir assinatura, com cargo e/ou função.

8 DO USO DA INTERNET

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria de órgão competente. Portanto, o CRP-06, em total conformidade com a legislação vigente, reserva-se o direito de monitorar, quando necessário, e, sempre que possível, registrar todos os *links* de acessos dentro de seu domínio institucional.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, *site*, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede.

Quanto ao uso propriamente dito da rede, fica definido que:

a) toda tentativa de alteração dos parâmetros de segurança, por qualquer usuária/o, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados à/ao colaboradora/colaborador e à/ao respectiva/o gestora/gestor;
b) o uso de qualquer recurso para atividades ilícitas poderá acarretar ações administrativas e as penalidades decorrentes de processos civil e criminal. Nesses casos, a instituição cooperará ativamente com as autoridades competentes;
c) a internet disponibilizada pela instituição às/aos suas/seus colaboradoras/es, independentemente de sua relação contratual, não pode ser utilizada para fins pessoais;
d) é proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, redes sociais, sites, salas de bate-papo, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha a surgir na internet;
e) as/os usuárias/os com acesso à internet somente poderão fazer o *download* de conteúdos ligados diretamente às suas atividades no CRP-06. Para isso, deverão providenciar o que for necessário para regularizar a licença e o registro de eventuais programas com a autorização a supervisão local;
f) esses *softwares* deverão passar previamente pelo crivo de segurança da equipe de TI. O uso, a instalação, a cópia ou a distribuição não autorizada de *softwares* que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos;
g) qualquer *software* não autorizado baixado poderá ser excluído pela TI;
h) as/os usuárias/os não poderão, em hipótese alguma, utilizar os recursos do CRP-06 para fazer o *download* ou distribuição de *software* ou dados pirateados;
i) o *download* e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) poderão ser realizados por usuárias/os que tenham atividades profissionais relacionadas a essas categorias. Para tal, serão criados grupos de segurança, cujas/os integrantes deverão ser definidos pelas/os respectivas/os gestoras/es, a fim de viabilizar esse acesso especial;
j) como regra geral, material de cunho sexual para pesquisa acadêmica não poderá ser exposto, armazenado, distribuído, editado, impresso ou gravado por meio de qualquer recurso;
    I. caso seja necessário, grupos de segurança deverão ser criados para viabilizar esse perfil de usuária/o especial e seus integrantes definidos pelas/os respectivas/os gestoras/es e informados ao setor de Tecnologia da Informação;
k) usuárias/os com acesso à internet não poderão efetuar *upload* e/ou *download* de qualquer *software* licenciado ao CRP-06 ou de dados de sua propriedade a seus/suas parceiras/os e clientes;
l) os serviços de comunicação instantânea (Skype, Meeting, Hangout pessoal e afins) serão inicialmente disponibilizados às/os usuárias/os e poderão ser bloqueados caso a/o ges-

tora/gestor requisite formalmente à coordenação de TI, uma vez que há ferramentas corporativas para comunicação disponíveis para todas as contas de *e-mail* (Zoom e InMail);

m) não é permitido acesso a *sites* de *proxy*. Quando necessário, solicitar à Unidade de Tecnologia da Informação;

n) toda e qualquer pesquisa institucional promovida eletronicamente, por meio de formulários, deverá ser previamente notificada à Unidade Jurídica, para que seja submetida a análise de conformidade com a LGPD (Lei Geral de Proteção de Dados) e, desta forma, ser verificado o atendimento às questões legais.

9 DOS DISPOSITIVOS MÓVEIS INSTITUCIONAIS

O CRP SP deseja facilitar a mobilidade e o fluxo de informação entre suas/seus usuárias/os. Por isso, permite a utilização de equipamentos portáteis, exclusivamente para a finalidade profissional.

Por "dispositivo móvel", entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, como: *notebooks, smartphones, tablets*, cartões de memória, HDs externos e *pen drives*.

O CRP SP, na qualidade de proprietário dos equipamentos e/ou serviços fornecidos, reserva-se o direito, caso seja necessário, de inspecioná-los a qualquer momento e realizar manutenção de segurança.

Portanto, a/o usuária/o assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na instituição, mesmo depois de terminado o vínculo institucional.

Ficam definidas, ainda, as seguintes diretrizes:

a) toda/o usuária/o deverá realizar periodicamente cópia de segurança (*backup*) dos dados de seu dispositivo móvel institucional, armazenando os dados em rede;
b) não é permitida a guarda de informações institucionais em dispositivos pessoais. Em caso de dúvidas quanto a este processo, entre em contato com a equipe de TI;
c) a TI só assegurará *backup* dos dados dispostos em rede institucional. Toda/o usuária/o deverá utilizar senhas de bloqueio automático para seu dispositivo móvel;
d) não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos;
e) a/o usuária/o será responsabilizada/o por manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da TI ou que estejam em desacordo com a política institucional do CRP SP;
f) a reprodução não autorizada dos *softwares* instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante;
g) é permitido o uso de rede *wi-fi* de locais conhecidos pela/o usuária/o, como sua casa, hotéis, fornecedores e clientes;
h) não é recomendado o compartilhamento de dados em redes *wi-fi* desconhecidas;
i) é responsabilidade da/o usuária/o notificar imediatamente sua/seu gestora/gestor direta/o e o departamento de Tecnologia da Informação do furto ou roubo de um dispositivo móvel fornecido pelo CRP SP. Além disso, deverá procurar a ajuda das autoridades policiais, registrando um boletim de ocorrência;
j) a/o usuária/o deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos pela má utilização e sua responsabilização por danos dolosos, diretos ou indiretos, presentes ou futuros, que venha a causar ao CRP SP e/ou a terceiros;
k) a/o usuária/o que desejar utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede do CRP SP deverá submeter previamente tais equipamentos ao processo de autorização de sua/seu superiora/superior imediata/o para liberação junto ao setor de Tecnologia da Informação.

9.1 DA TELEFONIA MÓVEL

Temos à disposição o serviço de telefonia móvel institucional para uso de usuárias/os previamente autorizadas/os pela diretoria. O serviço é restrito às atribuições funcionais.

O *e-mail* institucional da/o usuária/o será o identificador necessário para validação do aparelho.

A Unidade de TIC não se responsabiliza pela utilização de aplicativos e/ou conteúdo não condizente com os valores institucionais ou atribuições profissionais.

Em caso de avarias, furto, roubo ou perda do dispositivo, bem como *backup* e/ou garantia de dados, a/o colaboradora/colaborador é a/o responsável pela abertura do boletim de ocorrência e aviso ao departamento de TI, conforme termo de adesão, para que as medidas de segurança possam ser adotadas. Por isso, é recomendado que a/o colaboradora/colaborador peça periodicamente a realização de backup completo dos dados do aparelho em nuvem ou em *desktop/notebook*.

10 DO *BACKUP*

a) O *backup* de dados dos sistemas institucionais, rede, servidores e *e-mail* é de responsabilidade do setor de Tecnologia da Informação;
b) todos os *backups* devem ser automatizados por sistemas de agendamento que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de *backup*" (diariamente entre as 19h e as 5h). Esses são períodos de nenhum ou pouco acesso de usuárias/os e de processos automatizados aos sistemas de informática;
c) as antigas mídias de *backup* (como DAT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro e dentro do *datacenter*/Cedoc;
d) com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante, o tempo de vida e uso das mídias de *backup* deve ser monitorado e controlado pelas/os responsáveis e de acordo com as orientações do fabricante;
e) mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas;
f) os *backups* imprescindíveis, críticos, para o bom funcionamento do CRP SP exigem uma regra de retenção especial, conforme recomendação da ISO 27000, seguindo, assim, as determinações fiscais e legais existentes no país;
g) na situação de erro de *backup* ou restauração, é necessário que ele seja feito logo no primeiro horário disponível, assim que a/o responsável tenha identificado e solucionado o problema e respeitar a publicação de acordo de nível de serviço para a entrega da informação;
h) a restauração de dados, quando solicitada, poderá se dar em ambiente de teste e/ou mídia externa para não comprometer demais informações atualizadas;
i) demandas fora deste padrão deverão ocorrem em mídias físicas alternativas e de forma suplementar mediante a solicitação prévia de gestora/gestor.
j) não cabe à TI a responsabilidade por *backup*, formatação ou edição de dados computacionais disponíveis em outras formas de armazenamento que não os volumes da rede institucional.

11 DAS DISPOSIÇÕES FINAIS

Questões não previstas nesta Política deverão ser tratadas individualmente e pela Unidade de TIC do CRP-06 e encaminhados para deliberação da diretoria.

Há necessidade de revisões semestrais deste documento, a fim de mantê-lo atualizado às necessidades institucionais.

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna do CRP-06, ou seja, qualquer incidente de segurança será subentendido como ação contra o bem público e a responsabilidade regida pela autarquia.

ANEXO A

GUIAS DE SERVIÇOS E FERRAMENTAS

DO ARMAZENAMENTO EM NUVEM — NEXTCLOUD

O Nextcloud é a ferramenta institucional de código aberto para sincronização de arquivos, por meio do qual são compartilhados *softwares* para todas/os as/os usuárias/os, e fornece uma solução de compartilhamento e sincronização de arquivos segura e em conformidade com os servidores do CRP-06.

Serve para compartilhar um ou mais arquivos e pastas em seu computador e sincronizá-los com seu servidor Nextcloud, e será acessado pelo domínio nuvem.crpsp.org.br.

Os dados de *login* e senha serão ofertados pela Unidade de TI para as/os usuárias/os autorizados. É proibido o uso de outras formas de armazenamento em nuvem que não sejam por contas contratadas pelo CRP-06.

A interface da/o usuária/o Nextcloud contém os seguintes campos e funções:

a) **menu de seleção de aplicativos:** localizado no canto superior esquerdo, nele se encontram todos os aplicativos disponíveis em sua instância do Nextcloud. Clicar em um ícone de aplicativo irá redirecioná-lo para o aplicativo;
b) **campo "informações do aplicativo":** localizado na barra lateral esquerda, fornece filtros e tarefas associadas ao aplicativo selecionado. Por exemplo, ao usar o aplicativo Arquivos, pode-se acessar um conjunto especial de filtros para localizar rapidamente seus arquivos, como aqueles que foram compartilhados com você e aqueles que você compartilhou com outras pessoas. Outros aplicativos terão itens diferentes;
c) **visualização do aplicativo:** campo central principal na interface da/o usuária/o Nextcloud, que exibe o conteúdo ou os recursos da/o usuária/o para o aplicativo selecionado;
d) **barra de navegação:** localizada sobre a janela de visualização principal (a visualização do aplicativo), esta barra fornece um tipo de navegação estrutural que permite que você migre para níveis mais altos da hierarquia de pastas até o nível raiz (*home*);
e) **botão "novo":** localizado na barra de navegação, o botão "novo" permite criar novos arquivos, novas pastas ou fazer upload de arquivos;
f) **campo "pesquisar":** clique na lupa no canto superior direito para pesquisar arquivos e entradas do aplicativo atual;
g) **menu "contatos":** fornece uma visão geral de seus contatos e das/os usuárias/os em seu servidor. Dependendo dos detalhes fornecidos e dos aplicativos disponíveis, pode ser usado para iniciar uma chamada de vídeo diretamente com elas/eles ou enviar *e-mails*;
h) **botão visualização de grade:** botão formado por quatro pequenos quadrados que alterna a visualização da grade para pastas e arquivos;
i) **menu "configurações":** clique na imagem do seu perfil, localizada à direita do campo "pesquisar", para abrir o menu suspenso "configurações". A página de configurações fornece os seguintes recursos:
    I. *links* para baixar aplicativos de *desktop* e móveis;
    II. uso do servidor e espaço disponível;
    III. gerenciamento de senha;
    IV. configurações de nome, *e-mail* e foto do perfil;
    V. gerenciar navegadores e dispositivos conectados;
    VI. membras/os do grupo;
    VII. configurações de linguagem da interface;
    VIII. gerenciar notificações;
    IX. ID da nuvem federada e botões de compartilhamento de mídia social;
    X. gerenciador de certificados SSL/TLS para armazenamento externo;

XI. suas configurações de autenticação com dois fatores;
XII. informação da versão do Nextcloud.

Os arquivos Nextcloud, com a interface da *web* Nextcloud, servem para criar, visualizar, editar, excluir, compartilhar e recompartilhar arquivos.

A/o administradora/administrador do Nextcloud tem a opção de desativar esses recursos. Portanto, se algum deles estiver faltando no sistema, pergunte à/ao administradora/administrador do servidor.

Podem-se atribuir *tags* aos arquivos. Para criar *tags*, abra um arquivo na visualização "detalhes". Em seguida, digite suas *tags*. Para inserir mais de uma etiqueta, pressione a tecla "enter" depois de criar cada etiqueta. Todas as *tags* são *tags* do sistema e são compartilhadas por todas/os as/os usuárias/os no servidor Nextcloud.

Visualizar arquivos

É permitido exibir arquivos de texto não compactados, arquivos OpenDocument, vídeos e arquivos de imagem nos visualizadores incorporados do Nextcloud, clicando-se no nome do arquivo. Pode haver outros tipos de arquivo que você pode visualizar se o administrador do Nextcloud os tiver ativado. Se o Nextcloud não puder exibir um arquivo, ele inicia um processo de *download* e baixa o arquivo no seu computador.

Navegando dentro do Nextcloud

Navegar pelas pastas no Nextcloud é tão simples quanto clicar em uma pasta para abri-la e usar o botão voltar no seu navegador para passar para o nível anterior. O Nextcloud também fornece uma barra de navegação na parte superior do campo "arquivos" para uma navegação rápida.

Ícones de *status* do compartilhamento

Qualquer pasta compartilhada é marcada com o ícone de sobreposição "compartilhado". Os compartilhamentos de *links* públicos são marcados com um elo de corrente. As pastas não compartilhadas não são marcadas.

Selecionando arquivos ou pastas

Podem ser selecionados um ou mais arquivos ou pastas clicando-se nas caixas de seleção. Para selecionar todos os arquivos no diretório atual, clique na caixa de seleção localizada na parte superior da lista de arquivos.

Ao selecionar vários arquivos, você pode excluir todos eles ou baixá-los como um arquivo ZIP, usando os botões "excluir" ou "baixar" que aparecem na parte superior.

Filtrando a visualização de arquivos
A barra lateral esquerda na página "arquivos" contém vários filtros para classificar e gerenciar rapidamente seus arquivos.

Todos os arquivos

A visualização padrão; exibe todos os arquivos aos quais você tem acesso.

Favoritos

Arquivos ou pastas marcados com a estrela amarela.

Compartilhado com você

Exibe todos os arquivos compartilhados com você por outra/o usuária/o ou grupo.

Compartilhado com outras pessoas

Exibe todos os arquivos que você compartilhou com outras/os usuárias/os ou grupos.

Compartilhado por *link*

Exibe todos os arquivos compartilhados por você por meio de *link* público.

Movendo arquivos

Mover arquivos e pastas arrastando e soltando-os em qualquer diretório.

DOS PRODUTOS GOOGLE

O Google Workspace é um conjunto de soluções de nuvem que contribui para a melhor operação dos processos de trabalho da autarquia.

Promove a melhoria na produtividade e na colaboração, integrando inúmeras soluções disponíveis em qualquer lugar e em qualquer dispositivo.

Oferece proteção das informações da forma mais segura possível, passando por auditorias e cumprindo com os elevados padrões de segurança do setor.

A plataforma Google só será utilizada para gerar *links* de reuniões, em função da acessibilidade, e para fins de procedimentos da Comissão de Ética, Comissão de Orientação e Fiscalização, diretoria e secretaria, com a função de armazenar as gravações previstas nas normativas do CFP.

As contas contratadas ficarão sobre a responsabilidade das unidades acima citadas, não sendo permitido o compartilhamento de senhas e arquivos considerados confidenciais, como as gravações.

Oferece as seguintes ferramentas:

Docs

Para criar e editar documentos de texto, planilhas, tabelas e outros de forma *on-line* e *off-line*. Armazenamento seguro sincronizado com o Google Drive.

Drive

Para guardar documentos, fotos e planilhas de forma segura com o serviço de armazenamento e sincronização de arquivos.

Meet

Para videoconferências com segurança e acessibilidade.

Forms

Para coleta de pesquisas e informações por meio de formulários criados para pessoas ou grupos.

Sheets

Ferramenta para criação e edição de planilhas, gráficos e tabelas. Serviço sincronizado com Google Docs.

Agenda

Para criação de agendas compartilhadas que permitem ver quando outras pessoas estão disponíveis e programar reuniões com convites automáticos por *e-mail*.

DOS PRODUTOS ZIMBRA/IMMAIL

A plataforma Zimbra Mail é o domínio oficial e preferencial do CRP-06 e garante um *e-mail* seguro, aplicação de mensagens instantâneas individuais ou para grupos, realização de videoconferência com possibilidade de gravação e guarda das informações do *chat*, criação e compartilhamento de calendário e agenda, controle de tarefas, compartilhamento de documentos e vinculação com o armazenamento em nuvem.

Estes recursos estão disponíveis para plataformas de *webmail* e *desktop* e como aplicativos para dispositivos móveis (celulares e *tablets*).

Todos os recursos são de uso exclusivo para atividades institucionais, não sendo permitida a utilização e o compartilhamento para fins pessoais.

E-mail

O *e-mail* oferece a possibilidade de selecionar uma data e horário específicos para envio, por meio do recurso "enviar mais tarde" que fica localizado no *menu* suspenso.

Além da comunicação por *e-mail*, sua caixa de entrada do Zimbra é um ponto de partida para compartilhamento e colaboração de conteúdo, bate-papos e videoconferências. O cliente *web* responsivo do Zimbra pode ser acessado de qualquer lugar e em qualquer dispositivo, e permite uma transição perfeita entre os aplicativos do Zimbra. As/os usuárias/os podem redigir vários *e-mails* e alternar facilmente entre conversas com colegas de trabalho, edição de documentos ou revisão do calendário.

Se você se esqueceu de adicionar algo ao seu *e-mail* logo após clicar no botão "enviar" ou simplesmente se esqueceu de incluir um destinatário importante, o recurso de "desfazer envio" do Zimbra oferece alguns segundos para que você possa interromper o envio da mensagem para fazer quaisquer alterações. Os *e-mails* Zimbra também podem ser programados para envio em data e hora futuras.

Também é possível recuperar itens excluídos que foram para a lixeira, por até 30 dias. Porém, esse recurso tem que ser configurado pela/o usuária/o.

***Chat* integrado com dispositivo de mensagem instantânea — ImMail**

O ImMail é o dispositivo oficial e exclusivo do CRP-06 para troca de mensagens instantâneas para fins de avisos, recados e compartilhamento de *links* para reuniões.

É vedado o uso do ImMail para fins não institucionais ou passíveis de causar ações acusatórias, truculentas, difamatórios ou que produzam caos institucional.

Lista de tarefas

Para criar listas de tarefas já com detalhes de informações, por exemplo: datas de vencimento, prioridades, entre outros pontos.

Calendário

Para marcar uma reunião *on-line* abrindo o calendário e, por meio do "assistente de agendamento", verificar os dias e horários disponíveis de outras/os colaboradoras/es da sua empresa.

É possível utilizar atalhos de cópia, por meio do botão direito. Essa função permite um "copia e cola" dos compromissos (com as/os respectivas/os convidadas/os, anexos etc.).

Pasta para armazenamento em nuvem

Anexar arquivos direto do "Porta de Arquivos".
Salvar anexos de *e-mail* também no "Porta de Arquivos".
Carregar arquivos para acessá-los de forma instantânea no Zimbra Mail.

Pesquisa

Possibilita pesquisar o que se quiser na conta Zimbra (inclusive anexos), aproveitar os *menus* robustos para filtrar resultados de pesquisas, salvar cada pesquisa feita, se necessário, e ver os resultados (que não desaparecem quando você clica fora da janela).

Outros recursos (em quesitos mais técnicos e administrativos)

Implantar o *e-mail*, na nuvem, no local ou, ainda, como sistema híbrido.

Fazer o gerenciamento de recursos da/o usuária/o final, além de cotas, políticas de armazenamento, por meio de classe de serviço (CoS).

Ter proteção *anti-spam* e antivírus integrados.

Além disso, o *e-mail* Zimbra suporta IMAP/POP, CalDAV e CardDAV. A plataforma Zimbra também possui o Admin Console, que permite a administração da plataforma de qualquer lugar.

Controle e customização total

O *e-mail* Zimbra permite o gerenciamento técnico em nível de infraestrutura. O console de administração permite fazer o gerenciamento dos seus *e-mails*. Também oferece a interface de linha de comando, a conhecida CLI.

O Zimbra possui *anti-spam* e antivírus integrados na ferramenta. Defina suas próprias políticas de acesso, *anti-spam* e demais configurações.

Com o gerenciamento é possível criar restrição de acesso aos *e-mails* por horário, conforme você preferir.

O Zimbra permite controle total do sistema, podendo ter sua instalação customizada de acordo com a necessidade do seu negócio. Com o servidor dedicado, é possível mudar qualquer regra — como acesso, política de senha, controle *anti-spam* e muitas outras.

Acesso *mobile* e *desktop*

Para uma melhor experiência da/o usuária/o, é possível acessar seu ambiente Zimbra nas plataformas *desktop* e *mobile*.

Segurança

Segurança de dados e informações é outro ponto crucial para uma plataforma de *e-mail*. Nesse caso, você também pode ficar tranquilo, porque o Zimbra Mail possui recursos de alta segurança.

Estabilidade

A estabilidade pode ser comprovada em qualquer dispositivo móvel.

Compartilhamento de calendário

No ambiente colaborativo do Zimbra Mail, é possível compartilhar calendários. Dessa forma, todas/os as/os profissionais podem ver os horários disponíveis dos outros.

É possível sugerir outros horários clicando com o botão direito, no evento, para copiar e colar todas as informações (inclusive anexos) referentes a ele.

Interface intuitiva

Permite que as/os usuárias/os possam mudar facilmente de navegadores — além de *desktop*, celular e *tablet* — enquanto aproveitam toda a experiência de colaboração e *e-mail* estável.

Personaliza a interface da/o usuária/o com cores, fontes, logotipos e outros detalhes de sua preferência.

BRConselhos — BRC

Trata-se do sistema oficial do Sistema Conselhos de Psicologia. É uma solução integrada para gestão dos conselhos, que permite o controle de serviços gerenciais, financeiros e de fiscalização de forma remota, com garantia de segurança e integridade de acessos.
Apresenta as seguintes funcionalidades:

a) requerimentos *on-line*: as/os psicólogas/os inscritas/os no CRP SP têm à disposição um sistema de autoatendimento *on-line* que permite solicitar primeira inscrição ou inscrições secundárias, fazer atualização cadastral, solicitar declarações, cancelar inscrições, reativar inscrições suspensas ou canceladas, emitir certidão profissional, entre outras funcionalidades;
b) atendimento: o atendimento é a porta de entrada da/do psicóloga/o ou da pessoa jurídica para o CRP SP, oferecendo acesso aos serviços disponíveis, como CRP Acolhe, inscrição de pessoa física ou jurídica, renegociação de débitos, cancelamento, reativação, entre outros. Permite geração de relatórios;
c) COE: possibilita iniciar e acompanhar todas as fases dos processos éticos, mantendo os registros, fases processuais, documentos e resultados. Geração de relatórios, por processo, fase processual, registro de audiências, andamentos, mediação e pessoas mediadoras, entre outros;
d) COF: viabiliza o registro de controle das demandas de fiscalização, manutenção dos cadastros de temas, andamentos, fases processuais, questionários, documentos e relatórios;
e) financeiro: registro das anuidades, controle dos pagamentos via integração bancária, registro e disponibilização da posição financeira de cada uma das inscrições, processos de cobrança, manutenção da estrutura financeira, relatórios de cobrança, anuidades geradas, controle dos boletos, repasses ao CFP, Inscrição em Dívida Ativa (termo de inscrição e emissão de CDA — Certidão de Dívida Ativa);
f) jurídico: manutenção da dívida ativa, gestão e controle de processos, inclusão e exclusão de inadimplentes, andamento dos processos, relatórios dos processos, geração dos documentos e processos de cobrança;
g) contabilidade: manutenção da integração contábil, gerando os relatórios necessários para o processo de registro contábil dos resultados, como entradas efetivas, receitas por conta (mapa contábil), fundo de seção, fechamento contábil/financeiro.

Sistema Eletrônico de Informação (SEI!)

O sistema de gerenciamento de processos SEI! pode ser acessado por meio dos principais navegadores e permite o acesso remoto.

O sistema pretende garantir a eficiência dos processos sistematizados entre órgãos municipais, estaduais e federais; a variedade de formatos e tamanhos de documentos compatíveis; o controle de nível de acesso; e a tramitação simultânea de processos em múltiplas unidades. Por meio de uma interface intuitiva, a plataforma oferece ainda funcionalidades específicas, como controle de prazos, estatísticas da unidade, tempo do processo, pesquisa de inteiro teor, acompanhamento especial, textos-padrão, assinatura em bloco, organização de processos em bloco, e outros. Foi instituído pelo Decreto nº 8.539/2015.

> DECRETO Nº 8.539, DE 8 DE OUTUBRO DE 2015 — Dispõe sobre o uso do meio eletrônico para a realização do processo administrativo no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.

No âmbito do Executivo Federal, o extinto MPOG coordenou a implementação do Processo Eletrônico Nacional (PEN), com a adoção do Sistema Eletrônico de Informação (SEI!) pelos ministérios e outros órgãos vinculados ao Executivo federal até 2020.

O Processo Eletrônico Nacional (PEN) foi uma iniciativa conjunta de órgãos e entidades de diversas esferas da administração pública, com o intuito de construir uma infraestrutura pública de processos e documentos administrativos eletrônicos, objetivando a melhoria no desempenho dos processos do setor público, com ganhos em agilidade, produtividade, transparência, satisfação da/o usuária/o e redução de custos. Existiu até 2020. Introduziu práticas inovadoras no setor público: eliminação do uso de papel como suporte físico para documentos institucionais e disponibilização de informações em tempo real. Foi composto por algumas grandes ações, sendo o Sistema Eletrônico de Informações (SEI), desenvolvido pelo Tribunal Regional Federal da 4ª Região, a principal entrega.

O SEI! é uma plataforma que engloba um conjunto de módulos e funcionalidades que promovem a eficiência administrativa. A solução é cedida gratuitamente para instituições públicas e permite transferir a gestão de documentos e de processos eletrônicos administrativos para um mesmo ambiente virtual.

Vantagens

a) **portabilidade:** 100% *web* e pode ser acessado por meio dos principais navegadores do mercado;
b) **acesso remoto:** pode ser acessado remotamente por diversos tipos de equipamentos, como microcomputadores, *notebooks*, *tablets* e *smartphones* de vários sistemas operacionais. Isso possibilita que as/os usuárias/os trabalhem à distância;
c) **acesso de usuárias/os externos:** gerencia o acesso de usuárias/os externos, permitindo que tomem conhecimento dos documentos e, por exemplo, assinem remotamente contratos e outros tipos de processos;
d) **controle de nível de acesso:** gerencia a criação e o trâmite de processos e documentos restritos e sigilosos, conferindo o acesso somente às unidades envolvidas ou a usuárias/os específicos;
e) **tramitação em múltiplas unidades:** incorpora novo conceito de processo eletrônico, que rompe com a tradicional tramitação linear, inerente à limitação física do papel. Várias unidades podem ser demandadas, tomar providências e manifestar-se simultaneamente;

f) **funcionalidades específicas:** controle de prazos, ouvidoria, estatísticas da unidade, tempo do processo, base de conhecimento, pesquisa em todo teor, acompanhamento especial, inspeção administrativa, modelos de documentos, textos-padrão, sobrestamento de processos, assinatura em bloco, organização de processos em bloco, acesso externo etc.;

g) **sistema intuitivo:** estruturado com boa navegabilidade e usabilidade. *Software* público gratuito. Além disso, o acordo de cooperação técnica (ACT) assinado entre o CFP e o MPOG e a estrutura de TI já instalada ou em aquisição pelo CFP, conforme deliberação em Assembleia das Políticas, da Administração e das Finanças (Apaf), permite a adesão gratuita dos conselhos regionais ao PEN e ao SEI! para uso do sistema, mediante manifestação de interesse. Acordo já formalizado e utilizando uma estrutura única compartilhada;

h) **integração ao Sistema Conselhos de Psicologia:**

I. Elaboração de minutas de documentos e tramitações poderá ser executada por funcionárias/os do CRP a pedido de conselheiras/os (preferencialmente por *e-mail*, para registro);

II. *e-mails* com respostas de conselheiras/os poderão ser anexados aos processos por funcionárias/os;

III. conselheiras/os poderão assinar documentos elaborados por funcionárias/os e colocados em blocos internos, mesmo remotamente;

IV. reuniões e plenárias poderão ter suas pautas, com subsídios, organizadas e apresentadas integralmente via SEI!;

V. processos de diversas áreas/comissões poderão ser elaborados e tramitar entre os setores, com registro das deliberações e dos encaminhamentos executados por cada ator envolvido.

Sistema de passagens e diárias (Sispad)

O Sispad permite efetuar o controle das solicitações de viagens, autorizações das/os gestoras/es, emissão das passagens aéreas, pagamento das diárias e demais despesas com viagens custeadas pelo Conselho para conselheiras/os, diretoras/es, colaboradoras/es e convidadas/os.

O controle do sistema abrange todas as fases do processo e está integrado aos demais módulos desenvolvidos para as áreas financeira, administrativa e contábil.

A/O conselheira/conselheiro, colaboradora/colaborador ou trabalhadora/trabalhador deverá ingressar no Sispad com seu *login* e senha e seguir o Fluxo de Solicitação de Ressarcimento e Pagamento e da Prestação de Contas ao CRP-06.