CONSELHO REGIONAL DE CONTABILIDADE DO PARANÁ

RESOLUÇÃO Nº 891, DE 24 DE ABRIL DE 2026

INSTITUI A POLÍTICA DE SEGURANÇA EM RECURSOS HUMANOS.

O **CONSELHO REGIONAL DE CONTABILIDADE,** no uso de suas atribuições legais e regimentais,

CONSIDERANDO o Decreto nº 12.572, de 4 de agosto de 2025 que institui a Política Nacional de Segurança da Informação; e o Decreto nº 12.573, de 4 de agosto de 2025, que aprova a Estratégia Nacional de Segurança Cibernética;

CONSIDERANDO a Lei n.º 13.709, de 14 de agosto de 2018, que trata da Lei Geral de Proteção de Dados Pessoais (LGPD);

CONSIDERANDO as normas técnicas ABNT NBR ISO/IEC 27001:2022 (Sistema de Gestão de Segurança da Informação – SGSI) e ABNT NBR ISO/IEC 27002:2022 (Controles de Segurança da Informação);

CONSIDERANDO a Deliberação CRCPR n.º 028, de 11 de abril de 2022, que dispõe sobre a Política de Segurança da Informação do CRCPR; e a Portaria CRCPR n.º 021, de 8 de janeiro de 2024, que institui o Comitê de Tecnologia e Segurança da Informação no âmbito do CRCPR,

CONSIDERANDO a necessidade de definir princípios e diretrizes que garantam segurança da informação e a segurança cibernética, assegurando a adoção de controles técnicos e de procedimentos para validação dos sistemas desenvolvidos, mantidos, adquiridos ou em produção, de modo a preservar a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações tratadas pelo CRCPR.

R E S O L V E:

Art. 1º Fica instituída a Política de Segurança em Recursos Humanos no âmbito do Conselho Regional de Contabilidade do Paraná, nos termos do Anexo desta Resolução.

Art. 2° - Esta Resolução entrará em vigor na data de sua publicação no Diário Oficial do Estado do Paraná (DIOE-PR), revogando-se as disposições em contrário.

Contador **EVERSON LUIZ BREDA CARLIN**
Presidente
CO – CRCPR Nº 29.607/O

ANGELITA ROZA
CO – CRCPR Nº 64.278/O

ANTONIO MOACIR POZZOBON
CO – CRCPR Nº 20.423/O

ARIANE YUMI DE ALMEIDA ROCHA
CO - CRCPR Nº 40.667/O

CAROLINA ARAUJO DOS SANTOS FEIJÓ
CO – CRCPR Nº 69033/O

CESAR SOARES ZANIN
CO – CRCPR Nº 33.601/O

DANILO ALVES GRANI
CO – CRCPR Nº 56.387/O

EUNICE MARIA CAVALI DUARTE
CO – CRCPR Nº 34.322/O

FERNANDO ANTONIO BORAZO RIBEIRO
CO - CRCPR Nº 32.263/O

GERVALDO RODRIGUES CAMPOS
CO - CRCPR Nº 31.135/O

GISELE MARTINS MACHIOSKI
CO - CRCPR Nº 53.810/O

GLICÉRIO RAMPAZZO
CO – CRCPR Nº 35.574/O

JEFFERSON PAULO MARTINS
CO - CRCPR Nº 35.401/O

JOÃO GELÁSIO WEBER
TC - CRCSC Nº 10.131/O -TPR

JÚLIO RICARDO MORONA
CO – CRCPR Nº 48.431/O

MARCIA OGIDO HOKAMA
CO - CRCPR Nº 34.399/O

MARCIO JOSÉ ASSUMPÇÃO
CO – CRCPR Nº 36.207/O

MICHEL GULIN MELHEM
CO – CRCPR Nº 64.351/O

MIRIAM DA SILVA BRAZ
CO - CRCPR Nº 40.378/O

NELINHO KUKLA
CO - CRCPR Nº 50.194/O

RAFAEL ANTÔNIO DE LORENZO
CO - CRCPR Nº 41.346/O

RODINEI BONFADINI
CO - CRCPR Nº 42.621/O

ROSEMERE KIYOMI HAYASHI
CO – CRCPR Nº 35.176/O

RUBENS RICARDO POLIDO
CO - CRCPR Nº 49.198/O

SÉRGIO AUGUSTO DA PORCIÚNCULA JÚNIOR
CO - CRCRS Nº 69.409/O – TPR

SIMONE VANNI SOARES
CO - CRCPR Nº 36.620/O

Aprovada na 1.428ª Reunião Plenária de 2026, realizada em 24 de abril de 2026.

Documento assinado eletronicamente por **Everson Luiz Breda Carlin**, **Presidente**, em 24/04/2026, às 08:00, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Danilo Alves Grani**, **Vice-Presidente**, em 24/04/2026, às 08:07, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Michel Gulin Melhem**, **Vice-Presidente**, em 24/04/2026, às 08:08, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Rodinei Bonfadini**, **Vice-Presidente**, em 24/04/2026, às 08:09, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Cesar Soares Zanin**, **Conselheiro**, em 24/04/2026, às 08:12, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Ariane Yumi de Almeida Rocha**, **Vice-Presidente**, em 24/04/2026, às 08:14, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Fernando Antonio Borazo Ribeiro**, **Conselheiro**, em 24/04/2026, às 08:23, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Gisele Martins Machioski**, **Conselheira**, em 24/04/2026, às 08:29, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Carolina Araujo Dos Santos Feijó**, **Conselheira**, em 24/04/2026, às 08:33, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Rubens Ricardo Polido**, **Conselheiro**, em 24/04/2026, às 08:34, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Glicerio Rampazzo**, **Conselheiro**, em 24/04/2026, às 08:37, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Marcio José Assumpção**, **Conselheiro**, em 24/04/2026, às 08:39, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Sérgio Augusto da Porciúncula Júnior**, **Conselheiro**, em 24/04/2026, às 08:43, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Angelita Roza**, **Conselheira**, em 24/04/2026, às 08:44, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Miriam da Silva Braz**, **Conselheira**, em 24/04/2026, às 09:00, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Rafael Antonio de Lorenzo**, **Conselheiro**, em 24/04/2026, às 09:01, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Eunice Maria Cavali Duarte**, **Conselheira**, em 24/04/2026, às 09:02, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **João Gelásio Weber**, **Conselheiro**, em 24/04/2026, às 09:02, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Marcia Ogido Hokama**, **Conselheira**, em 24/04/2026, às 09:02, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Julio Ricardo Morona**, **Conselheiro**, em 24/04/2026, às 09:11, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Rosemere Kiyomi Hayashi**, **Vice-Presidente**, em 24/04/2026, às 10:00, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Simone Vanni Soares**, **Conselheiro**, em 24/04/2026, às 10:03, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Antonio Moacir Pozzobon**, **Conselheiro**, em 24/04/2026, às 10:04, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Gervaldo Rodrigues Campos**, **Conselheiro**, em 27/04/2026, às 18:19, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Jefferson Paulo Martins**, **Vice-Presidente**, em 28/04/2026, às 10:05, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1317542** e o código CRC **FCC93608**.

ANEXO I

POLÍTICA DE SEGURANÇA EM RECURSOS HUMANOS

CAPÍTULO I
DA INSTITUIÇÃO, DO OBJETIVO E DA APLICAÇÃO

Art. 1º Fica instituída a Política de Segurança em Recursos Humanos no âmbito do Conselho Regional de Contabilidade do Paraná.

Art. 2º Esta Política tem por objetivo assegurar que os empregados ocupantes de cargos efetivos, terceirizados e estagiários:

I – compreendam suas responsabilidades com relação ao cumprimento da Política de Segurança da Informação, Segurança Cibernética e demais políticas do CRCPR;

II – estejam conscientes das ameaças relativas à segurança da informação;

III – atuem de forma ativa no apoio às diretrizes e controles estabelecidos pelo CRCPR;

IV – reportem imediatamente qualquer violação ou suspeita de descumprimento das Políticas.

Art. 3º A Política de Segurança em Recursos Humanos é o documento que estabelece princípios, conceitos, diretrizes e define os papéis e as responsabilidades que devem ser observadas na seleção e contratação de pessoal, conscientização, no processo de educação e treinamento em segurança da informação e segurança cibernética e na instauração de processo administrativo disciplinar, naquilo que for cabível.

Art. 4º Esta norma se aplica a todos os empregados ocupantes de cargos efetivos, terceirizados e estagiários.

Art. 5º Esta norma não substitui a Política de Gestão de Pessoas adotada pelo CRCPR, mas a complementa quanto aos aspectos de segurança da informação e segurança cibernética.

Art. 6º A elaboração e atualização deste documento é de responsabilidade do Comitê de Tecnologia e Segurança da Informação.

CAPÍTULO II
DOS TERMOS E DAS DEFINIÇÕES

Art. 7º Para os efeitos desta Política, são estabelecidos os seguintes conceitos e definições:

I – Ameaça: qualquer circunstância ou evento com o potencial de causar incidente indesejado que pode resultar em dano para um sistema ou instituição;

II – Análise de Risco: uso sistemático de informações de identificação de fontes para estimar o risco;

III – Atividade: ação ou conjunto de ações executadas por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

IV – Ativos de informação: qualquer dispositivo de software ou hardware que agrega valor ao negócio e compõe a infraestrutura de rede de dados do CRCPR, assim como também os locais onde se encontram estes dispositivos, gestão do pessoal que a eles possuem acesso, além dos processos envolvidos na gestão e operacionalização dos ativos de informação;

V – Ciberativos: hardwares, softwares, redes, dispositivos, aplicações, serviços, sistemas e dados utilizados para processar, armazenar ou transmitir informações por meio eletrônico ou digital;
VI – Ciberameaça: circunstância ou evento, resultante de ciberofensa, com potencial para impactar, de forma adversa, indivíduos ou organizações, incluídos seus ativos, suas operações, suas funções, sua imagem ou sua reputação;
VII – Cibercrime: crime praticado contra ou por meio de ciberativos;
VIII – Ciberefeito: dano, permanente ou temporário, indisponibilidade ou limitação da operação, total ou parcial, ou mudança de comportamento de ciberativo ou não, resultante de ciberofensa;
IX – Ciberincidente: ciberofensa combinada ao ciberefeito real ou potencial resultante de ciberofensa;
X – Ciberofensa: conjunto de ações adotadas no ciberespaço em oposição a ciberativo;
XI – Cibersegurança: conjunto de ferramentas, salvaguardas, diretrizes, abordagens de gestão de riscos, ações, treinamentos, melhores práticas, garantias e tecnologias, entre outras medidas usadas para proteger o ciberespaço e os ciberativos do usuário e da organização;
XII - Ciber-risco: possibilidade de ocorrência de ciberincidente;

XIII – Colaboradores: são todos os empregados efetivos, terceirizados e estagiários;

XIV – Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;

XV – Disponibilidade: propriedade de estar acessível e utilizável sob demanda por um usuário autorizado;

XVI – Integridade: propriedade de salvaguarda da exatidão e a completude da informação contra alterações, intencionais ou acidentais, em seu conteúdo ou durante seu processamento;

XVII – Segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações;

XVIII – Sigilo: segredo de conhecimento restrito a pessoas credenciadas, proteção contra revelação não autorizada;

XIX – Sistema de informação: aplicação da tecnologia da informação que dá apoio às atividades de determinada área de conhecimento, visando otimizar as operações, o gerenciamento e a decisão, trabalhando os dados e transformando-os em informação;

XX - Tecnologia da informação: conjunto de ciberativos destinados ao processamento de sistemas e de dados; e

XXI – Usuários: os empregados ocupantes de cargos efetivos, terceirizados, e estagiários que acessam ou utilizam informações custodiadas ou de propriedade do CRCPR.

CAPÍTULO III

DAS DIRETRIZES

Art. 8º Para assegurar que os empregados ocupantes de cargos efetivos, terceirizados e estagiários compreendam as suas responsabilidades na proteção da informação e da segurança cibernética, deverão ser adotadas as seguintes diretrizes e procedimentos:

I – disponibilizar políticas, normas e procedimentos de segurança da informação e demais políticas, compiladas no Manual de Integração, quando da nomeação e contratação de empregados, terceirizados, estagiários;

II – promover divulgação contínua desses documentos, assegurando que todos os usuários conheçam os riscos e suas obrigações;

III – realizar treinamentos e atualizações periódicas sobre a segurança da informação;

IV – comunicar à Coordenadoria de TIC toda movimentação de pessoal, incluindo contratações, desligamentos, transferências e alterações no quadro efetivo, bem como início e término de contratos de terceirizados e estagiários;

V – coletar assinatura do Termo de Responsabilidade desta Política de Segurança em Recursos Humanos (Anexo I), durante o processo de contratação;

VI – manter atualizados e arquivados os Termos de Responsabilidade;

VII – promover campanhas de conscientização para fortalecer a cultura de segurança;

VIII – avaliar, periodicamente, o nível de maturidade do CRCPR nos aspectos relacionados à segurança da informação;

IX – instaurar processo administrativo disciplinar para apuração de responsabilidades e aplicação das sanções previstas em regulamentações internas e legislação em vigor, em caso de descumprimento ou violação, pelo usuário, das regras previstas nas políticas, normas e procedimentos de segurança da informação do CRCPR.

CAPÍTULO IV
DOS PROCEDIMENTOS E DAS RESPONSABILIDADES

Art. 9º Este capítulo define os responsáveis e um conjunto de procedimentos que deverão ser seguidos para garantir a segurança da informação do CRCPR.

Art. 10º Cabe a Divisão Contábil, Financeira e RH e/ou Fiscal de contrato:

I – incluir, nos editais de concurso público, em observância aos princípios do art. 37 da Constituição Federal, a exigência de apresentação do Termo de Responsabilidade relativo à Política de Segurança da Informação, Cibersegurança e Acesso Lógico (Anexo I), como requisito para investidura no cargo;

II - receber, do candidato habilitado e convocado, o Termo de Responsabilidade (Anexo I), arquivando-o nos autos funcionais juntamente com os demais documentos de contratação;

III – disponibilizar, para análise e ciência, a Política de Segurança da Informação ao estudante ou profissional selecionado, respectivamente, para ocupar a vaga de estagiário e terceirizado;

IV – recepcionar, o Termo de Responsabilidade (Anexo I), assinado pelos estagiários e terceirizados no ato da contratação, arquivando-o nos autos;

V – atualizar, e coletar assinatura do Termo de Responsabilidade, sempre que houver atualização do normativo, mantendo os documentos arquivados;

VI – elaborar, implementar e divulgar o Plano Anual de Treinamento de Tecnologia da Informação e Cibersegurança, em conjunto com a Comitê de Tecnologia e Segurança da Informação e Divisão de Governança, Riscos, Compliance e LGPD, para desenvolver as competências gerenciais e técnicas necessárias à operacionalização da governança, gestão e atualização tecnológica;

VII – inserir, no Plano Anual de Treinamento, evento voltado a atualização das políticas e procedimentos de segurança da informação e cibersegurança a todos os usuários;

a) o treinamento deverá ocorrer pelo menos uma vez por ano e sempre que houver atualização ou criação de novas políticas ou procedimentos;

VIII – instruir o processo de contratação e de realização dos eventos de capacitação sobre segurança da informação e Cibersegurança, incluindo:

a) inscrição dos participantes;

b) divulgar e convocar os colaboradores;

c) acompanhar a realização do evento;

IX – promover treinamento de integração para novos contratados, em até 30 (trinta) dias do início da atividade, para orientar sobre as políticas, normas e procedimentos de segurança da informação e cibersegurança;

X – comunicar à Coordenadoria de TIC sempre que ocorrerem admissões, desligamentos e movimentações de empregados, terceirizados e estagiários;

XI – encaminhar à Comissão de Conduta do CRCPR quaisquer usuários que violarem esta Política e as políticas, normas e procedimentos de segurança da informação e cibersegurança, ainda que mera suspeita;

XII – à Comissão de Conduta compete receber as representações de denúncias de violações a esta Política e a políticas, normas e procedimentos de segurança da informação e cibersegurança, instaurar e instruir processo administrativo disciplinar e apurar responsabilidades, com base nos normativos internos aplicáveis.

Art. 11º Cabe ao Comitê de Tecnologia e Segurança da Informação:

I – avaliar o nível de maturidade dos usuários do CRCPR nos aspectos relacionados à segurança da informação e cibersegurança:

a) elaborar os quesitos que deverão compor a pesquisa de comportamento dos usuários;

b) formatar a pesquisa com as orientações para preenchimento;

c) encaminhar a pesquisa à Coordenadoria de Tecnologia e Segurança da Informação, para aplicação aos usuários;

d) avaliar o resultado da pesquisa de comportamento dos usuários e apresentar proposição de melhoria das políticas, normativos e procedimentos.

II – pesquisar no mercado, a oferta de cursos e eventos sobre segurança da informação e cibersegurança, solicitar proposta de preços, analisar as propostas, definir a realização do treinamento e submetê-las ao Divisão de RH para instrução do processo de contratação e/ou execução;

III – analisar e aprovar o projeto da campanha para divulgação, sensibilização e conscientização das políticas, suas normas e procedimentos;

IV – analisar a efetividade das ações implementadas voltadas ao estabelecimento da cultura e ampliação do nível de maturidade;

V – analisar as proposições apresentadas pelos usuários para alteração das políticas, normas ou procedimentos;

VI – impedir a execução operacional de uma atividade crítica, exclusivamente, por único empregado;

VII – prestar esclarecimento imediato aos usuários sobre dúvidas relacionadas à política, às normas e aos procedimentos;

Art. 12º Cabe à Coordenadoria de TIC:

I – divulgar, aplicar, tabular e apresentar o resultado da pesquisa, elaborada pelo Comitê de Tecnologia e Segurança da Informação, para aferir o nível de maturidade dos usuários do CRCPR nos aspectos relacionados à segurança da informação e cibersegurança:

a) divulgar e orientar os usuários sobre os procedimentos para preenchimento da pesquisa de comportamento dos usuários;

b) aplicar a pesquisa, aprovada pelo Comitê de Tecnologia e Segurança da Informação;

c) consolidar os dados e apresentar o resultado ao Comitê para proposição de melhorias;

II - identificar a necessidade e propor a contratação de treinamentos específicos aos empregados lotados na Coordenadoria de TIC para manter o alto nível de maturidade;

III - desativar ou liberar acessos aos sistemas e equipamentos, conforme previstos nas políticas e nos procedimentos relacionados à segurança da informação e cibersegurança, sempre que houver admissão, desligamento ou movimentação de empregado, terceirizado e estagiário;

IV - restringir o acesso de profissionais terceirizados aos computadores, sistemas, servidores, serviços internos, intranet, correio eletrônico e à rede do CRCPR somente àquilo que se fizer essencial para prestação de seus serviços e de forma especificada em documento de contrato vigente;

V – assegurar que as informações internas sejam compartilhadas apenas por meios oficiais de comunicação do CRCPR e, em situações excepcionais, avaliar previamente a forma adequada de fazê-lo.

a) são meios oficiais de comunicação do CRCPR:

- Contas de email com o domínio "crcpr.org.br";
- Ferramenta de mensagens instantâneas e videoconferências Microsoft Teams vinculada a uma conta oficial do CRCPR;
- Ferramenta de mensagens instantâneas Whatsapp vinculada a um número de telefonia celular oficial do CRCPR;
- Ferramenta de videoconferências Zoom Meetings em reuniões oficiais programadas pelo CRCPR;
- Demais ferramentas do pacote Microsoft 365 vinculadas a uma conta oficial do CRCPR;
- Aplicações oficiais fornecidas por terceirizados, devidamente autorizados e com contratos vigentes, que possuam canais de comunicação e/ou abertura de chamados nos quais há necessidade de fornecimento de informação sobre a solicitação, observada a LGPD Lei nº 13.709/2018 especialmente em seus capítulos IV, V e VII;
- Aplicações oficiais fornecidas por terceirizados, devidamente autorizados e com contratos vigentes, que possuam armazenamento próprio em nuvem ou em sua estrutura física (On-Premises), observada a LGPD Lei nº 13.709/2018 especialmente em seus capítulos IV, V e VII.

VI – prestar esclarecimentos imediatos aos usuários sobre dúvidas relacionadas à política, às normas e aos procedimentos.

Art. 13º Cabe à Gerência de Comunicação do CRCPR:

I – desenvolver o projeto da campanha para divulgação, sensibilização e conscientização das políticas, normas e dos procedimentos de segurança da informação e cibersegurança, submetendo-o ao Comitê de Tecnologia e Segurança da Informação para aprovação, observando:

a) o projeto da campanha deverá ser elaborado anualmente para execução durante o ano em curso;

b) a campanha deve incentivar e engajar os usuários para a prática da segurança da informação e cibersegurança em suas atividades;

c) deve contemplar a conscientização dos usuários quanto às ameaças externas, tais como vírus, interceptação de mensagens e dados, grampos, fraudes e tentativas que ensejem o roubo de senhas e que possam afetar ou ameaçar a segurança do CRCPR;

d) a campanha deve abordar as penalidades em caso de descumprimento das políticas, normas e procedimentos;

e) incluir na campanha o Dia da Segurança da Informação "30 de novembro" no CRCPR;

f) executar a campanha de divulgação das políticas, normas e procedimentos de segurança da informação e cibersegurança aprovada pelo Comitê de Tecnologia e Segurança da Informação.

Art. 14º Cabe aos gestores:

I – adotar postura exemplar em relação à segurança da informação e cibersegurança, servindo como modelo de conduta para os colaboradores sob sua gestão;

II – cumprir e fazer cumprir esta Política e demais políticas, normas e procedimentos;

III – promover cultura de segurança institucional, fazendo com que os colaboradores sob sua gestão compreendam as necessidades das medidas adotadas e incorporem o conceito de que todos os usuários são responsáveis por garantir a proteção da informação;

IV – prestar esclarecimento imediato aos colaboradores sob sua gestão sobre dúvidas relacionadas à política, às normas e aos procedimentos de segurança da informação e cibersegurança;

V – adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade às diretrizes desta política e demais normativos correlatos;

VI – autorizar o acesso e definir o perfil e a mudança de perfil do usuário junto a Coordenadoria de TIC;

VII – propor melhorias e alterações nas políticas, normas e nos procedimentos de segurança da informação e cibersegurança;

VIII – identificar a necessidade e propor à Divisão de RH a contratação de novos cursos para os empregados sob sua gestão, visando manter o alto nível de maturidade em segurança da informação e cibersegurança;

IX – compartilhar com as demais divisões e os empregados sob sua gestão informações necessárias à produção de conhecimentos relacionados com as atividades de segurança da informação e

cibersegurança;

X – monitorar continuamente os cenários de interesse do CRCPR no que se refere à segurança da informação, de modo a proporcionar suporte adequado ao desenho das funções da instituição;

XI – relatar prontamente à Coordenadoria de TIC qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento e presença de vírus;

XII – relatar para seu superior hierárquico e à Coordenadoria de TIC o surgimento da necessidade de um novo *software* para o desenvolvimento de suas atividades;

XIII – reportar à Comissão de Conduta do CRCPR, ainda que por mera suspeita, qualquer usuário que violar esta Política e demais políticas, normas e procedimentos de segurança da informação e cibersegurança;

Art. 15º Cabe aos empregados ocupantes de cargos efetivos, terceirizados e estagiários:

I – cumprir as políticas, normas e procedimentos que tratem da segurança a informação e cibersegurança;

II – tomar ciência de todo material disponibilizado pelo CRCPR sobre o tema;

III – assinar, obrigatoriamente, o Termo de Responsabilidade relativo a Política de Segurança da Informação cibersegurança (Anexo I) e demais normativos correlatos;

IV – estar sempre atualizado e ciente das políticas, normas e procedimentos vigentes;

V – adquirir conhecimento necessário para a correta utilização dos recursos relacionados à segurança da informação e cibersegurança;

VI – buscar esclarecimentos à chefia imediata ou à Coordenadoria de TIC sempre que houver dúvidas;

VII – participar das campanhas, eventos, cursos ou atualizações promovidas pelo CRCPR;

VIII – proteger ativos de informação contra acesso, divulgação, transmissão, compartilhamento, modificação, destruição ou interferência não autorizadas, conforme disposto nas Políticas relacionadas a LGPD do CRCPR;

IX – atuar de forma responsável, pessoal e intransferível, na utilização dos recursos, tecnológicos ou não, disponibilizados pelo CRCPR para o desempenho de suas atividades na prestação de serviços para o Conselho;

X – adotar a prática de não abordagem e não discussão em ambientes públicos e áreas expostas sobre assuntos relacionados ao trabalho;

XI – comunicar ao gestor imediato ou a Comissão de Conduta do CRCPR ou à Coordenadoria de TIC ou ao Comitê de Tecnologia e Segurança da Informação, quaisquer eventos ou incidentes potenciais ou reais que causem riscos à segurança da informação e cibersegurança, ou ainda sua mera suspeita;

XII – relatar à Coordenadoria de TIC qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento ou presença de vírus;

XIII – informar ao gestor imediato e à Coordenadoria de TIC o surgimento da necessidade de nova ferramenta ou *software*s;

XIV – denunciar à Comissão de Conduta eventuais violações a esta Política e as políticas, normas e procedimentos de segurança da informação e cibersegurança, ainda que mera suspeita;

XV – apresentar sugestões de melhorias para as políticas, normas e procedimentos de segurança da informação e cibersegurança;

XVI – responder pelo prejuízo ou dano que vier a provocar ao CRCPR ou a terceiros, em decorrência da não obediência às diretrizes e normas;

XVII – atuar de forma responsável, pessoal e intransferível, pelo sigilo, privacidade e uso de senhas de acesso aos recursos computacionais, não podendo estas serem compartilhadas, divulgadas, anotadas em papel ou em sistema visível ou de acesso não protegido:

a) as senhas utilizadas para acesso aos recursos são pessoais, intransferíveis e devem ser escolhidas atendendo às melhores práticas definidas na Política de Controle de Acesso Lógico do Conselho Regional de Contabilidade do Paraná;

b) troca imediata das senhas, nos casos de perda de sigilo ou mesmo suspeita.

XVIII – utilizar crachá de identificação durante a permanência nas dependências do CRCPR;

XIX – acompanhar toda e qualquer manutenção preventiva ou corretiva realizada em equipamentos sob sua responsabilidade;

XX – desenvolver outras atividades correlatas visando à efetiva segurança da informação e cibersegurança.

Art. 16º É vedado aos empregados ocupantes de cargos efetivos, terceirizados e estagiários:

I – conectar na rede interna do CRCPR equipamentos não autorizados;

II – abrir ou executar arquivos de origem desconhecida;

III – acessar informação institucional que não seja explicitamente autorizada ou não vinculada às suas atividades profissionais;

IV – transportar informações confidenciais do CRCPR sem as devidas autorizações e proteções e em qualquer meio, como CD, DVD, HD, *pen drive*, compartilhamento em nuvem, papel, entre outros;

V – alterar normas padronizadas dos ativos;

VI – acessar e divulgar informações que contenham material obsceno, apologia ao fanatismo, práticas religiosas, político-partidário, qualquer forma de discriminação ou material que, explícita ou

implicitamente, se refira à conduta imoral;

VII – fazer cópias de materiais da internet, inclusive desenhos, artigos, gráficos e fotografias, sem autorização do proprietário ou citação da fonte;

VIII – alimentar-se próximo aos servidores de rede, equipamentos e estações de trabalho;

IX – fazer cópia não autorizada de *softwares* adquiridos ou desenvolvidos pelo CRCPR;

X – instalar ou desabilitar qualquer ferramenta ou aplicativo nos recursos tecnológicos de propriedade do CRCPR sem a expressa homologação autorização da Coordenadoria de TIC;

XI – Utilizar sistemas e aplicativos instalados localmente ou que funcionem de forma on-line através da internet que não tenham sido expressamente homologados, autorizados e disponibilizados pela Coordenadoria de TIC;

XII – utilizar recursos tecnológicos fornecidos pelo CRCPR para fins particulares.

CAPÍTULO V
DAS VIOLAÇÕES E SANÇÕES

Art. 17º O descumprimento desta Política e das demais políticas, normas e procedimentos de segurança da informação e cibersegurança constitui falta contratual, e os empregados ocupantes de cargos efetivos, terceirizados e estagiários estarão sujeitos às penalidades definidas nos normativos que tratam do processo administrativo disciplinar, podendo acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, assegurando aos envolvidos o contraditório e a ampla defesa.

Art. 18º O não cumprimento desta Política e das demais políticas, normas e procedimentos de segurança da informação e cibersegurança poderá implicar:

i) Para empregados:

a) Comunicação de descumprimento: Será encaminhado ao funcionário, por e-mail, comunicado informando o descumprimento da norma, com a indicação precisa da violação praticada. Cópia desse comunicado permanecerá arquivada junto a Divisão de Recursos Humanos na respectiva pasta funcional do infrator;

b) Advertência ou suspensão: A pena de advertência ou suspensão será aplicada, por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade;

c) Demissão por justa causa: A demissão por justa causa poderá ser aplicada nas hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho (CLT), alíneas *"a"* a *"f"*, quando configuradas as condutas ali tipificadas.

II - Estagiários, prestadores de serviços e outros

a) o término antecipado do contrato de estágio e prestação de serviços, bem como, nos termos da legislação aplicável, sanções civis e penais e eventuais ressarcimentos por danos causados ao

CRCPR.

Art. 19º Além das sanções, caso o gestor entenda necessário e viável, poderá aplicar aos empregados ocupantes de cargos efetivos, terceirizados e estagiários, mediante Termo de Ajuste de Conduta, uma medida educativa, que consistirá na realização de cursos, *workshops* e treinamentos, que serão disponibilizados pelo CRCPR.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 20º Os casos omissos desta Política serão resolvidos pelo Comitê de Tecnologia e Segurança da Informação do CRCPR.

ANEXO II

TERMO DE RESPONSABILIDADE
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, CIBERSEGURANÇA e ACESSO LÓGICO

Pelo presente termo, eu, _____, declaro ter conhecimento da Política de Segurança da Informação, cibersegurança E Acesso Lógico do Conselho Regional de Contabilidade do Paraná, disponível para consulta no site do CRCPR aba Governaça - LGPD.

Declaro que estou recebendo uma conta com privilégios adequados ao exercício das atividades que executo, a qual será utilizada somente para tal fim.

Declaro estar ciente de que minhas ações serão monitoradas nos termos da Política de Segurança da Informação, cibersegurança e acesso lógico do CRCPR e de que qualquer alteração será de minha responsabilidade, feita a partir de minha identificação, autenticação e autorização.

Estou ciente, ainda, que serei responsável pelo dano que possa causar em caso de descumprimento da Política de Segurança da Informação, cibersegurança e demais políticas do CRCPR, ao realizar uma ação de iniciativa própria de tentativa quanto à modificação da configuração, física ou lógica, dos recursos computacionais sem a permissão da área competente.

Curitiba/PR, 24 de abril de 2026.