CONSELHO REGIONAL DE CONTABILIDADE DO PARANÁ

RESOLUÇÃO CRCPR Nº 892, DE 24 DE ABRIL DE 2026.

APROVA A POLÍTICA DE SEGURANÇA DE INFORMAÇÃO DO CONSELHO REGIONAL DE CONTABILIDADE DO PARANÁ (CRCPR).

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

CONSIDERANDO a Lei n.º 13.709, de 14 de agosto de 2018, que trata da Lei Geral de Proteção de Dados Pessoais, assim com a legislação correlata à proteção de Dados Pessoais;

CONSIDERANDO o Decreto nº 12.572, de 4 de agosto de 2025 que institui a Política Nacional de Segurança da Informação;

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 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 estabelecer, no âmbito interno, as responsabilidades pertinentes à Segurança da Informação, assegurando a proteção de dados pessoais, dos ativos informacionais e dos recursos tecnológicos;

RESOLVE:

Art. 1º - Aprovar a Política de Segurança de Informação do Conselho Regional de Contabilidade do Paraná nos termos do Anexo desta Resolução.

Art. 2º - Esta Resolução entrará em vigor na data de sua publicação no Diário Oficial do Estado do Paraná (DIOE-PR), restando revogadas as demais disposições sobre o tema, inclusive a Deliberação **CRCPR Nº 028/2022**.

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

GISELE MARTINS MACHIOSKI

CO - CRCPR Nº 31.135/O

GLICÉRIO RAMPAZZO
CO – CRCPR Nº 35.574/O

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

MARCIA OGIDO HOKAMA
CO - CRCPR Nº 34.399/O

MICHEL GULIN MELHEM
CO – CRCPR Nº 64.351/O

NELINHO KUKLA
CO - CRCPR Nº 50.194/O

RODINEI BONFADINI
CO - CRCPR Nº 42.621/O

RUBENS RICARDO POLIDO
CO - CRCPR Nº 49.198/O

SIMONE VANNI SOARES
CO - CRCPR Nº 36.620/O

CO - CRCPR Nº 53.810/O

JEFFERSON PAULO MARTINS
CO - CRCPR Nº 35.401/O

JÚLIO RICARDO MORONA
CO – CRCPR Nº 48.431/O

MARCIO JOSÉ ASSUMPÇÃO
CO – CRCPR Nº 36.207/O

MIRIAM DA SILVA BRAZ
CO - CRCPR Nº 40.378/O

RAFAEL ANTÔNIO DE LORENZO
CO - CRCPR Nº 41.346/O

ROSEMERE KIYOMI HAYASHI
CO – CRCPR Nº 35.176/O

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

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 08:11, 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 **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 **Rubens Ricardo Polido**, **Conselheiro**, 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 **Carolina Araujo Dos Santos Feijó**, **Conselheira**, 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 08:38, 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 08:44, 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 **Angelita Roza**, **Conselheira**, em 24/04/2026, às 08:45, 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 09:01, 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 **Rafael Antonio de Lorenzo**, **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 **João Gelásio Weber**, **Conselheiro**, em 24/04/2026, às 09:03, 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 **Eunice Maria Cavali Duarte**, **Conselheira**, em 24/04/2026, às 09:03, 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 **Marcia Ogido Hokama**, **Conselheira**, em 24/04/2026, às 09:04, 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 **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 10:01, 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 **Simone Vanni Soares**, **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 **Antonio Moacir Pozzobon**, **Conselheiro**, em 24/04/2026, às 10:06, 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.

ANEXO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação do CRCPR estabelece princípios, diretrizes e controles destinados a proteger os dados pessoais e demais ativos informacionais contra acessos não autorizados, incidentes acidentais ou ilícitos de destruição, perda, alteração, divulgação ou qualquer forma de tratamento inadequado, em conformidade com o art. 46 da Lei nº 13.709/2018 (LGPD).

Este documento está alinhado à Política Nacional de Segurança da Informação – PNSI (Decreto nº 12.572/2025), que define a segurança da informação como dever do Estado e orienta a proteção dos dados, dos ativos informacionais, do ambiente físico e eletrônico, bem como do pessoal envolvido no ciclo de vida da informação; e à Estratégia Nacional de Cibersegurança – E-Ciber (Decreto nº 12.573/2025), que estabelece diretrizes para prevenção, detecção, resposta e resiliência em segurança cibernética no país.

A Política também adota as boas práticas e controles internacionalmente reconhecidos pelas normas 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), as quais orientam a implementação de medidas técnicas, administrativas e organizacionais adequadas para proteção das informações tratadas pela instituição.

Com vistas à garantia da qualidade, continuidade e confiabilidade na prestação dos serviços públicos, torna-se indispensável a formalização desta Política, que define parâmetros claros para o uso adequado de recursos tecnológicos e estabelece condutas consideradas inadequadas ou proibidas.

Para fins desta Política, consideram-se “serviços e recursos” os equipamentos, sistemas e meios tecnológicos tais como computadores, impressoras, contas de e-mail institucional sob o domínio crcpr.org.br, rede corporativa, acesso à Internet, ferramentas de comunicação e demais ativos tecnológicos, disponibilizados aos colaboradores que nos termos desta são definidos como: conselheiros, representantes, empregados, estagiários, prestadores, terceiros e visitantes.

As normas definidas neste documento não constituem lista exaustiva e poderão ser atualizadas periodicamente para refletir avanços tecnológicos, alterações regulatórias ou necessidades institucionais. Quaisquer mudanças serão comunicadas oportunamente aos usuários.

Em caso de dúvidas sobre condutas que possam representar violação desta Política, o usuário deverá contatar previamente a Divisão de TIC pelo e-mail informatica@crcpr.org.br, a fim de obter orientação e garantir o uso seguro dos recursos.

Havendo necessidade de advertência ou aplicação de medida disciplinar, a situação será encaminhada a Comissão de Conduta e a divisão de Recursos Humanos para acompanhamento e registro, nos termos das normas internas.

As diretrizes estabelecidas nesta Política encontram-se organizadas nos tópicos apresentados a seguir:

A seguir, apresentamos as normas mencionadas. Ressaltamos que qualquer ação não expressamente autorizada ou permitida constitui violação à Política tratada nesta Resolução. Todos os usuários são responsáveis por garantir a segurança das informações às quais têm acesso ao utilizar a Rede institucional.

1. UTILIZAÇÃO DAS INFORMAÇÕES E RECURSOS

A concessão de acesso às informações será realizada por meio dos controles formais de gestão de usuários, considerando a necessidade de uso, o princípio do menor privilégio e o grau de sigilo aplicável a cada informação.

O acesso a dados pessoais e demais informações protegidas será autorizado exclusivamente aos usuários que necessitem desses dados para o desempenho de suas atividades institucionais. Cada usuário deverá acessar e tratar apenas as informações e ambientes para os quais tenha permissão expressa. Tentativas deliberadas de acesso não autorizado constituem violação grave e sujeitam o infrator às medidas administrativas cabíveis.

As credenciais e permissões de acesso são individuais e intransferíveis. O acesso aos sistemas ocorrerá mediante identificação e autenticação do usuário, devendo as credenciais serem mantidas sob sigilo e protegidas contra uso indevido.

Os recursos de tecnologia disponibilizados pelo CRCPR destinam-se exclusivamente ao uso institucional. É vedada a utilização para fins pessoais, salvo em situações excepcionais e justificadas. Nessas hipóteses, a autorização deverá ser previamente concedida pela chefia imediata, com registro do motivo, data e período de uso, e comunicação à área de TIC para fins de monitoramento e controle.

2. UTILIZAÇÃO DA REDE

A utilização da rede corporativa do CRCPR deverá observar os princípios da segurança da informação, da gestão de riscos, da responsabilidade individual, e da preservação da integridade, disponibilidade e confidencialidade dos ativos tecnológicos, em conformidade com a legislação vigente que reforça a prevenção, detecção e resposta a incidentes, bem como com as boas práticas.

Esse tópico visa definir as normas de utilização da rede que englobam desde o login, manutenção de arquivos no servidor e tentativas não autorizadas de acesso.

a) É expressamente proibida qualquer tentativa de obtenção de acesso não autorizado, incluindo fraudes de autenticação, exploração de vulnerabilidades, acesso a dados ou sistemas não permitidos ou testes não autorizados de segurança de rede ou servidores internos e de outras redes;

b) É proibida qualquer tentativa de interferência nos serviços de outro usuário, servidor ou da rede, tais como ataques de negação de serviço, sobrecarga deliberada de servidores, exploração de falhas ou qualquer ação que comprometa o funcionamento da infraestrutura;

c) Não é permitido o uso de programas, scripts, comandos ou ferramentas destinadas a interromper, alterar, monitorar ou interferir em sessões ou atividades de outros usuários;

d) Ao se ausentar do local de trabalho, o usuário deve encerrar programas, bloquear a estação de trabalho ou efetuar logout. As estações serão configuradas com bloqueio automático após período de inatividade, conforme diretrizes de segurança;

e) O usuário deve manter seu diretório pessoal organizado, evitando o acúmulo de arquivos desnecessários que possam comprometer o desempenho dos sistemas;

f) É proibido armazenar, transmitir ou processar materiais de natureza pornográfica, racista, discriminatória ou ilícita nos recursos tecnológicos da instituição;

g) Não é permitido criar, mover ou excluir arquivos fora das pastas autorizadas ou realizar ações que possam comprometer o desempenho dos sistemas. As áreas de armazenamento são definidas conforme tabela abaixo:

Compartilhamento	**Utilização**
Diretório **T:**	Arquivos Pessoais inerentes ao CRCPR
Diretório **F:\user\nome_da_divisão**	Arquivos da divisão em que trabalha
Diretório **F:\geral** ou **F:\user\geral**	Arquivos temporários ou de compartilhamento geral
Diretório OneDrive (Office 365)	Arquivos pessoais inerentes ao CRCPR

Tabela 1

Em algumas áreas, podem existir compartilhamentos adicionais conforme necessidade funcional.

h) A pasta *GERAL* (ou equivalente) não deve ser utilizada para armazenamento de documentos sigilosos ou sensíveis;

i) É obrigatório armazenar arquivos institucionais exclusivamente no servidor do CRCPR, uma vez que não há garantia de backup no OneDrive;

j) A pasta *GERAL* sofrerá limpeza semanal para evitar acúmulo desnecessário de arquivos;

k) A instalação ou remoção de softwares só poderá ser realizada pela área de TIC; toda solicitação deverá ser formalizada preferencialmente via Helpdesk ou e-mail institucional;

l) É proibida a abertura física de equipamentos; qualquer manutenção deverá ser realizada exclusivamente pela Divisão de TIC;

m) Não é permitida a alteração de configurações de rede, inicialização das máquinas ou demais parâmetros que possam causar instabilidade ou riscos aos sistemas;

n) A instalação de softwares ou hardwares sem autorização da equipe técnica é proibida;

o) É vedado realizar downloads de filmes, músicas, imagens ou quaisquer conteúdos provenientes de fontes ilegais ou de pirataria. Esses sites são monitorados pela TIC;

p) É proibida a utilização de dispositivos pessoais de armazenamento; quando necessário, a TIC fornecerá equipamentos adequados e seguros;

q) Não é permitida a utilização de aplicativos de mensagens instantâneas pessoais (ex.: WhatsApp Web, Skype) nas estações de trabalho, exceto quando autorizado à equipe gestora que utiliza dispositivo pessoal para atividades profissionais;

r) As portas USB permanecem bloqueadas por padrão. Caso seja necessária sua liberação, deverá haver autorização formal da chefia e registro junto à equipe de TIC. É proibido carregar smartphones nas portas USB das estações de trabalho;

s) Quando necessário transferir arquivos de grande volume, deverá ser utilizada conta institucional no OneDrive (Office 365), fornecida pela equipe de TIC.

3. COMPUTAÇÃO PESSOAL E MÓVEL

O tratamento de dados pessoais e demais informações institucionais do CRCPR deverá ocorrer exclusivamente em equipamentos corporativos.

a) Os dados pessoais e demais informações tratadas nos sistemas do CRCPR devem ser acessadas e processadas prioritariamente em equipamentos corporativos devidamente configurados e gerenciados pela área de Tecnologia da Informação e Comunicação (TIC), de modo a garantir a segurança da informação e a conformidade com a legislação vigente. Em situações excepcionais, poderá ser admitida a utilização de dispositivos pessoais para o tratamento de dados institucionais, desde que haja autorização formal da chefia imediata, com comunicação prévia à área de TIC, e observância das diretrizes de segurança da informação estabelecidas pelo CRCPR;

b) As estações de trabalho são de uso individual, configuradas conforme o perfil de acesso e as permissões necessárias ao desempenho das funções do colaborador. A utilização da estação de trabalho de outro usuário somente poderá ocorrer mediante autorização formal da chefia, acompanhada de registro enviado à área de TIC contendo motivo, data e período de uso;

c) É obrigatório o bloqueio da estação de trabalho sempre que o usuário se ausentar, mesmo que temporariamente, como medida de prevenção contra acesso indevido, em conformidade com as boas práticas de segurança.

4. POLÍTICA DE SENHAS

As senhas constituem mecanismo essencial de autenticação e controle de acesso, devendo ser gerenciadas de forma a garantir a **proteção contra acessos não autorizados**, em conformidade com as boas práticas previstas. A utilização e o gerenciamento de senhas devem observar os seguintes requisitos:

a) As senhas temporárias fornecidas pela área de TIC devem ser alteradas pelo usuário imediatamente no primeiro acesso. A redefinição periódica obrigatória ocorrerá a cada 42 (quarenta e dois) dias, conforme política institucional vigente;

b) As senhas são sigilosas, individuais e intransferíveis. O usuário é responsável por preservar sua confidencialidade, adotando práticas seguras de criação, armazenamento e uso, bem como monitorando sua conta para evitar acessos indevidos;

c) Todas as ações executadas por meio das credenciais de um usuário são de sua inteira responsabilidade. Assim, o usuário deve assegurar que sua senha permaneça secreta, evitando qualquer divulgação ou exposição;

d) Para garantir segurança adequada, as senhas devem obedecer aos seguintes critérios mínimos:

- Não utilizar informações pessoais fáceis de serem descobertas (telefone, endereço, datas de nascimento etc.);
- Conter no mínimo sete caracteres;
- Incluir letras maiúsculas e minúsculas;
- Conter números e caracteres especiais;
- Incluir pelo menos um caractere especial.

5. GESTÃO DE IDENTIDADES

A política de gestão de identidades tem por finalidade assegurar que o acesso às informações e aos sistemas do CRCPR ocorra de forma controlada, proporcional, rastreável e compatível com as atribuições funcionais de cada colaborador, em conformidade com os princípios de governança, necessidade de acesso, menor privilégio e segregação de funções.

a) Princípios Gerais

O acesso a dados pessoais, informações sensíveis e sistemas corporativos será concedido somente quando estritamente necessário ao desempenho das funções do colaborador, observando o princípio do menor privilégio.

Todos os acessos devem ser formalmente autorizados, registrados e periodicamente revisados, conforme boas práticas estabelecidas.

b) Perfis de Acesso

Gerente Operacional e Equipe de TIC: terão acesso a todos os dados pessoais do banco de dados do CRCPR e às informações necessários às suas atividades, incluindo ambientes técnicos que demandem administração, monitoramento ou suporte especializado.

Gerentes e Coordenadores: terão acesso aos dados pessoais e operacionais relacionados ao seu setor, na extensão necessária à supervisão e à execução das atividades institucionais.

c) Alteração de Cargo ou Lotação

Em casos de mudança de função, setor ou desligamento, os acessos deverão ser revisados, ajustados ou revogados imediatamente, garantindo que o colaborador mantenha apenas os privilégios coerentes com seu novo perfil.

d) Controle de Acessos

Os acessos aos sistemas corporativos serão concedidos com base na descrição de cargo, nas funções exercidas e nas necessidades informacionais da Divisão do colaborador.

Cada acesso será realizado mediante uso individual de credenciais autenticadas, garantindo rastreabilidade e responsabilização, conforme determina a PNSI no tocante à governança da informação.

O processo de concessão, alteração, suspensão ou revogação de acessos será conduzido pela área de TIC, mediante solicitação formal da chefia e aprovação do responsável pelo ativo, em conformidade com a governança preconizada pela E-Ciber.

6. UTILIZAÇÃO DE E-MAIL

O uso do correio eletrônico institucional do CRCPR deve observar os princípios de **segurança da informação, proteção de dados pessoais, prevenção contra ameaças cibernéticas e uso responsável**, em conformidade com a **Política Nacional de Segurança da Informação – PNSI**, que determina a necessidade de controle e proteção de informações no ambiente digital, e com a **Estratégia Nacional de Cibersegurança – E-Ciber,** que orienta quanto à segurança das comunicações e mitigação de riscos cibernéticos. As diretrizes também seguem as boas práticas de comunicação segura previstas nos controles da **ISO/IEC 27002:2022**, especialmente sobre uso aceitável, proteção contra malware, manipulação de informações, prevenção de engenharia social e controle de acesso.

A conta de e-mail corporativo é destinada exclusivamente ao uso institucional, sendo vedada sua utilização para fins pessoais.

Os usuários devem estar cientes de que o tráfego de e-mail ocorre em ambiente público e sujeito a riscos inerentes (atrasos, falhas, exposição a conteúdo malicioso). Assim, é fundamental a adoção de práticas seguras ao enviar, receber e gerenciar mensagens.

Regras de Utilização

a) O e-mail deve ser utilizado com responsabilidade, evitando perturbações a terceiros, linguagem inadequada ou mensagens excessivamente longas e frequentes;

b) Mensagens devem ser enviadas apenas a destinatários que desejam recebê-las; solicitações de interrupção de envio devem ser prontamente atendidas;

c) É proibido o envio de grande volume de mensagens (spam), incluindo publicidade, mala direta, campanhas políticas ou qualquer conteúdo que possa comprometer o desempenho da rede ou causar transtornos a outros usuários. Envio de e-mail para grande volume de destinatários deverá ser feito exclusivamente pela Divisão de TIC;[WL1] [MJ2]

d) É proibido reenviar ou propagar mensagens em cadeia, independentemente do consentimento de destinatários;

e) É proibido enviar fotos ou documentos institucionais via aplicativos ou mídias de celulares pessoais. Em caso de recebimento ou necessidade de envio não sendo possível a utilização da Plataforma de Comunicação Instantânea institucional, o usuário deverá transferir imediatamente o arquivo para o equipamento corporativo e excluir definitivamente a mídia do dispositivo móvel;[WL3] [MJ4]

f) Documentos e informações institucionais devem ser enviados exclusivamente por meio do e-mail corporativo ou das ferramentas oficiais de comunicação interna como Plataforma de Comunicação Instantânea e Microsoft Teams;

g) Evite enviar mensagens a grupo superior a dez destinatários simultaneamente. É proibido sobrecarregar usuários, sistemas ou servidores por meio de *mail bombing* ou anexos excessivamente grandes;

h) O CRCPR poderá bloquear automaticamente:

- mensagens com anexos que comprometam o desempenho ou a segurança da rede;
- mensagens enviadas para destinatários ou domínios considerados de risco ou que afetem o fluxo operacional;

i) É proibido falsificar informações do cabeçalho do remetente;

j) É vedado o uso de linguagem inadequada em mensagens profissionais, incluindo abreviações informais, gírias ou termos ofensivos;

k) O usuário deve manter sua caixa de e-mail organizada, evitando acúmulo excessivo de mensagens e anexos que prejudiquem o desempenho das ferramentas corporativas;

l) Para confirmar o recebimento de mensagens críticas, recomenda-se utilizar recursos como solicitações de aviso de "leitura" e "recebimento";

m) O usuário não deve abrir anexos enviados por remetentes desconhecidos ou suspeitos;

n) Não abra arquivos com extensões executáveis (.bat, .exe, .src, .lnk, .com) sem absoluta certeza de sua legitimidade;

o) Desconfie de e-mails com assuntos incomuns ou em idioma inesperado, pois podem constituir tentativas de phishing ou disseminação de malware (ex.: casos históricos como *ILOVEYOU*);

p) Recomenda-se o uso de assinatura padronizada, contendo nome, função e telefone comercial, conforme modelo oficial definido pela Diretoria;

Imagem Exemplo

Nome do Funcionário

Função

Telefone Comercial

q) O CRCPR disponibiliza ferramenta de AntiSpam, que permite ao usuário gerenciar e revisar mensagens filtradas, acessando o site http://antispam.crcpr.org.br. Dúvidas devem ser direcionadas à Divisão de TIC;

r) Recomendações para melhorar a comunicação por e-mail:

- Usar adequadamente os campos "Para", "Cc" e "Cco".
  - **Para:** responsável pela ação ou interessado na informação
  - **Cc:** envolvido diretamente no assunto (pessoas em Cc não têm obrigação de responder)
  - **Cco:** use para manter a lista de destinatários em sigilo
- Utilizar "Ação:" no início do assunto quando houver solicitação ou prazo.
  - Ex.: "Ação: realizar empenho da empresa XYZ. Prazo 7/julho."
- Estruturar mensagens em três partes: objetivo, ação requerida, histórico.
  - **Objetivo:** breve resumo do objetivo, para criar o contexto da mensagem.
  - **Ação requerida e prazo:** informar claramente, se possível em destaque.
  - **Histórico e informações adicionais**: devem vir no final, preferencialmente em anexos se for muita informação.
- Evitar parágrafos longos, cores excessivas e textos em CAIXA ALTA.
- Evitar anexos grandes e uso do recurso "Responder a todos".
- Conferir destinatários, assunto e conteúdo antes do envio.
  - **Certifique-se que:** todos os destinatários precisam receber a mensagem;
  - **O campo assunto inicia com "Ação:"** (quando houver uma ação);
  - **O conteúdo** da mensagem está claro e o formato está adequado.

7. UTILIZAÇÃO DE ACESSO À INTERNET

A utilização da Internet no âmbito do CRCPR deve ser realizada de forma responsável, segura e estritamente vinculada às atividades institucionais, observando os princípios de **gestão de riscos, proteção da informação, uso aceitável** e **segurança cibernética.** A Divisão de TIC poderá aplicar **bloqueios preventivos ou corretivos** sempre que a navegação comprometer o desempenho da rede, a continuidade das operações ou a segurança dos ativos institucionais.

Normas de Utilização da Internet

a) É proibido utilizar os recursos do CRCPR para download, distribuição ou uso de softwares, arquivos ou dados **não legalizados**, sem licença válida ou sem autorização institucional;

b) É proibida a divulgação de informações confidenciais ou sensíveis do CRCPR em sites, fóruns, listas de discussão, redes sociais ou salas de bate-papo, ainda que de forma acidental ou não intencional, sujeitando o infrator as penalidades previstas nas políticas e procedimentos internos e ou na legislação aplicável;

c) A Internet poderá ser utilizada para fins pessoais **somente** no horário de almoço ou fora do expediente, desde que não viole esta Política nem comprometa a segurança, desempenho ou conformidade do ambiente tecnológico;

d) Apenas programas diretamente relacionados às atividades do CRCPR poderão ser baixados. O usuário deve garantir a regularização de licenças e registros sempre que aplicável;

e) É proibido realizar upload de softwares licenciados ao CRCPR ou de arquivos institucionais para qualquer ambiente externo sem autorização prévia da Divisão de TIC;

f) A Divisão de TIC poderá bloquear:

- Arquivos que comprometam o uso de banda ou a estabilidade operacional;
- Domínios que possam prejudicar o desempenho, segurança ou conformidade da rede;

g) A navegação na Internet poderá ser monitorada e registrada. Relatórios de acesso poderão ser gerados e divulgados internamente quando necessário, em conformidade com as normas de segurança;

h) É obrigatória a utilização **exclusiva** dos navegadores homologados pelo setor de TIC (Mozilla Firefox, Microsoft Edge ou Google Chrome), devidamente configurados e atualizados;

i) É proibido o uso de softwares ou serviços de comunicação instantânea para fins pessoais, incluindo Skype, Yahoo Messenger, Facebook Messenger e similares.

j) É proibida a utilização de programas de compartilhamento *peer-to-peer* (P2P), como Kazaa, Morpheus, BitTorrent e equivalentes;

k) Não é permitido o acesso a sites de relacionamento ou redes sociais que não tenham finalidade institucional (ex.: Facebook, Instagram, Gazag e similares);

l) O acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas ou outros considerados inadequados é bloqueado, e tentativas de acesso poderão ser monitoradas;

m) É proibida a utilização de serviços de streaming, tais como rádios online e plataformas similares, salvo quando autorizados para fins institucionais.

8. UTILIZAÇÃO DE IMPRESSORAS

A utilização das impressoras corporativas deverá ocorrer de forma responsável, observando práticas de uso eficiente e adequado dos recursos institucionais, garantindo a preservação de materiais, a organização do ambiente e o bom funcionamento dos equipamentos compartilhados. Sempre que possível, deve-se priorizar a geração de documentos digitais em formato PDF; quando isso não for viável, aplicam-se as normas abaixo.

Normas de Utilização das Impressoras

a) Antes de enviar qualquer documento para impressão, o usuário deve verificar se a impressora está ligada, abastecida de papel e, quando conectada a um computador específico, se o equipamento também se encontra ligado;

b) Caso a impressão seja malsucedida, o papel que puder ser reaproveitado deverá ser recolocado na bandeja. Se o papel puder ser utilizado como rascunho, o usuário deverá levá-lo para sua mesa. Se não houver utilidade, deve ser descartado adequadamente;

c) É proibido deixar impressões incorretas, esquecidas ou não retiradas sobre a impressora, mesas próximas ou gaveteiros. Documentos esquecidos devem ser recolhidos e descartados de forma adequada, especialmente quando contiverem informações sensíveis;

d) Caso a impressora emita folhas em branco, estas deverão ser recolocadas corretamente na bandeja, salvo quando apresentarem defeitos que impeçam o reaproveitamento;

e) Ao verificar que o papel da impressora está no final, o usuário deverá reabastecê-la, evitando interrupções nas impressões de outros colaboradores e reduzindo o acúmulo de tarefas na fila;

f) A impressora colorida deverá ser utilizada **exclusivamente para versões finais** de documentos ou materiais que realmente demandem impressão colorida, sendo vedado seu uso para testes, rascunhos ou impressões desnecessárias;

g) Sempre que possível, deve-se optar pela impressão em **frente e verso**, como forma de promover o uso racional do papel e reduzir desperdícios.

9. MANUSEIO E ARMAZENAMENTO DE DOCUMENTAÇÃO FÍSICA

O manuseio e o armazenamento de documentos físicos no CRCPR devem observar práticas que assegurem a proteção da informação, a continuidade operacional, a integridade dos registros e a prevenção de acessos não autorizados, garantindo aderência às normas institucionais e às boas práticas de segurança da informação.

Normas de Manuseio e Armazenamento

a) Todos os procedimentos relacionados à proteção, guarda, acesso e continuidade do uso de informações físicas devem ser formalizados e documentados, permitindo sua execução mesmo na ausência do responsável direto;

b) Documentos em meio físico que contenham dados pessoais ou dados pessoais sensíveis devem ser armazenados em envelopes ou pastas e guardados em gavetas ou armários fechados, observando-se controles de acesso adequados;

c) É proibido deixar documentos contendo dados pessoais, informações sigilosas ou registros institucionais expostos sobre mesas ou superfícies desprotegidas;

d) Impressões de documentos devem ser limitadas ao estritamente necessário;

e) Folhas que possam ser reaproveitadas como rascunho devem ser separadas adequadamente; folhas contendo informações confidenciais, pessoais ou estratégicas devem ser descartadas por meio de trituradores de papel ou métodos de destruição segura;

f) Documentos físicos com dados pessoais ou informações sensíveis devem ser armazenados em locais trancados, com acesso restrito, formalizado por meio de termo de responsabilidade firmado entre a gestão e o colaborador autorizado;

g) O arquivamento de documentos físicos deve seguir rigorosamente a Classificação Documental e a Tabela de Temporalidade, garantindo conformidade com regras de retenção, guarda, eliminação e gestão documental.

10. VERIFICAÇÃO DA UTILIZAÇÃO DA POLÍTICA DE UTILIZAÇÃO DA REDE

Para assegurar o cumprimento das normas de uso da rede e garantir a proteção dos ativos tecnológicos do CRCPR, a instituição poderá adotar mecanismos de monitoramento, inspeção e controle, em conformidade com as diretrizes nacionais de segurança da informação e cibersegurança.

Normas de Verificação

a) O CRCPR poderá implantar e operar softwares, sistemas e ferramentas de monitoramento capazes de registrar, analisar e armazenar informações sobre o uso da Internet, tráfego de rede e atividades realizadas nas estações de trabalho, para fins de segurança, auditoria e prevenção de incidentes;

b) O CRCPR poderá inspecionar arquivos armazenados na rede institucional, inclusive em discos locais das estações de trabalho e áreas privadas de armazenamento, quando necessário para verificar conformidade com esta Política, preservar a segurança ou apurar potenciais violações;

c) A infraestrutura de rede do CRCPR conta com softwares e hardwares de segurança, como firewalls, sistemas de detecção e prevenção de intrusão, filtros de conteúdo e demais camadas defensivas, destinados a proteger a integridade dos dados, a disponibilidade dos serviços e a confidencialidade das informações.

11. CADASTRO DO PONTO ELETRÔNICO

O registro de ponto eletrônico é obrigatório no âmbito do CRCPR, em conformidade com a Portaria nº 671/2021 do Ministério do Trabalho e Emprego, que estabelece os requisitos legais para sistemas eletrônicos de controle de jornada e sua autenticidade, inviolabilidade e precisão.

O CRCPR utiliza sistema externo para a gestão do ponto eletrônico, garantindo integridade, rastreabilidade e segurança das informações, em atendimento aos princípios da governança da informação.

Normas de Registro de Ponto

a) Na contratação de empregados sob o regime da CLT, será realizado o cadastramento eletrônico do colaborador no sistema de ponto;

b) O sistema de ponto eletrônico poderá ser acessado por meio do endereço eletrônico fornecido pela Divisão de RH;

c) Todos os registros de entrada, saída e intervalos devem ser efetuados exclusivamente no sistema oficial, sendo proibida a utilização de meios informais ou alternativos;

d) O CRCPR poderá realizar verificações, auditorias e controles de integridade nos registros, conforme permitido pela legislação e pelas normas internas de segurança da informação.

DO TRATAMENTO DE DADOS DOS COLABORADORES

O CRCPR realiza o tratamento de dados pessoais de seus colaboradores e de seus dependentes exclusivamente para finalidades legítimas, específicas e necessárias, relacionadas à gestão de pessoas, ao cumprimento de obrigações legais e regulatórias e à administração de benefícios, em conformidade com a LGPD.

A seguir são descritas as categorias de dados pessoais tratadas, bem como suas respectivas finalidades e bases legais aplicáveis.

DADOS COLETADOS	FINALIDADE	BASE LEGAL

Foto 3x4 recente e colorida*	**Documentos para fins de admissão de empregado aprovado em concurso público.**	Art 7º, I, da Lei nº 13.709/2018.
Cópia do RG		
Cópia do CPF		
CTPS - Carteira de trabalho e Previdência Social		
Carteira de Habilitação		
Cópia de Certidão de nascimento ou casamento (conforme o caso)		
Título de eleitor e certidão de quitação eleitoral		
Certificado de reservista		
Cópia de documento de inscrição no PIS/PASEP		
Cópia do cartão Transporte		
Consulta a Qualificação Cadastral no portal do eSocial		
Certidão do distribuidor criminal da justiça estadual e federal		
Certidão negativa de antecedentes criminais		
Declaração de bens		
Currículo detalhado		
Comprovação de escolaridade		
Registro no órgão de classe (quando for necessário)		
Comprovante de endereço atualizado		
Certidão de nascimento dos filhos menores de 18 anos*		
Termo de Guarda do filho menor que estiver sob tutela;		
Dados bancários para pagamento do salário		
Exame Admissional*		
Nome completo	**Dados para emissão do contrato de trabalho**.	Art 7º, I, da Lei nº 13.709/2018.
Número da carteira de trabalho (CTPS) com o nº da série		
Função a ser exercida		
Remuneração inicial de acordo com tabela salarial do PCCS do CRCPR		
Horário a ser cumprido		
Data de início do contrato		
Regime de Contrato		
Nome completo, inclusive o nome social	**Dados para Inclusão no sistema de folha de pagamento, obrigações acessórias e eSocial.**	Art 7º, I, da Lei nº 13.709/2018, Art.13 e seguintes do Decreto-Lei nº 5.452/1943, Decreto nº 76.900/1975, Instrução Normativa RFB nº 1.919/2019, Decreto nº 8.373/2014, Portaria Conjunta SEPRT / RFB nº 82/2020, Portaria Conjunta SEPRT / RFB nº 76/2020, Lei nº 9.528/97, Lei nº 8.036/90, Lei nº 8.212/91 e Lei nº 8.213/91.
Data de nascimento		
Nome do pai e mãe		
Gênero		
Estado Civil		
Raça/Cor*		
Naturalidade e Nacionalidade		
Endereço residencial completo		
Endereço eletrônico		
Carteira de identidade (RG)		
Cadastro de pessoa física (CPF)		
Carteira nacional de habilitação (CNH)		
Carteira de trabalho (CTPS) - física ou digital		
Número do programa de integração social (PIS/PASEP)		
Nível de instrução ou de escolaridade		
Certificado de reservista		
Título de eleitor e certidão de quitação eleitoral		

Dados bancários com número do banco, agência e conta corrente Cópia carteira do conselho profissional (caso exigido em edital) Cargo/Função a ser exercida Certidão de casamento (se casado) Certidão de nascimento dos filhos* Cadastro de pessoa física (CPF) dos filhos*		
Nome completo Foto 3x4* Cargo/Função Matrícula Data de admissão Lotação	**Dados para identificação pessoal no crachá**.	Art 7º, V, da Lei nº 13.709/2018.
Nome completo Número do RG e CPF Número de registro funcional no CRCPR Data de nascimento Data de admissão Divisão da lotação Horário de trabalho Função a ser exercida	**Dados para inclusão no Portal do RH.**	Art 7º, V, da Lei nº 13.709/2018.
Nome Completo Matrícula Data de admissão Função exercida Departamento Horário de trabalho	**Dados do Espelho do Cartão Ponto e relatório de ocorrências**.	Art 7º, V, da Lei nº 13.709/2018.
Nome completo Matrícula Data de nascimento Número do RG e CPF Endereço Data de admissão	**Dados para inclusão no sistema do prestador de serviços de Medicina Ocupacional**.	Art 7º, I e V da Lei nº 13.709/2018, NR 7 e NR 9.
Nome completo Matrícula Nome do pai e mãe Data de nascimento Número do RG e CPF Endereço Data de admissão Cópia Carteira de Trabalho ou Ficha de Registro Declaração de saúde (inclusão fora de prazo de renovação de ctr)* Nome do dependente (quando solicitado pelo funcionário)* Nome do pai e mãe (quando solicitado pelo funcionário) Data de nascimento (quando solicitado pelo funcionário)* Grau de parentesco (quando solicitado pelo funcionário) Cópia da certidão de nascimento (quando solicitado pelo funcionário)*	**Dados e cópia de documentos para inclusão no sistema do prestador de serviços de Plano de Saúde.**	Art 7º, I, da Lei nº 13.709/2018.

Nome completo Matrícula Data de nascimento Número do RG e CPF Data de admissão	**Dados para inclusão nos sistemas de benefícios como o vale refeição/alimentação e vale transporte (quando solicitado pelo funcionário).**	Art 7º, I e V, da Lei nº 13.709/2018.
Realização de exames referentes a medicina ocupacional: ASO, PPRA, PCMSO e PPP*	**Documentos para fins de manutenção no emprego e demissão.**	Art. 11,II,"a", DA Lei 13/709/2018, Portaria ME/SEPRT nº 6.734/2020, NR-7, NR-9.
Atestado médico*	**Afastamento do Trabalho.**	Art. 11,II,"a", DA Lei 13/709/2018, Art. 473 da CLT, Art. 6º da Lei nº 605/49 e CF/88.
Dados bancários	**Para realização do pagamento de verbas trabalhistas.**	Art.7º, V, da Lei nº 13.709/2018.

13. DAS VIOLAÇÕES E SANÇÕES

O não cumprimento pelo funcionário das normas ora estabelecidas neste Documento (¨Políticas de Segurança¨), seja isolada ou cumulativamente, poderá ensejar, de acordo com a infração cometida, as seguintes punições:

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.

Por tratar-se o CRCPR de autarquia federal, criada pelo Decreto Lei nº 9.295/1996, a aplicação de penalidades observará o devido Processo Administrativo Disciplinar (PAD), assegurando-se a formação de comissão específica, o contraditório e a ampla defesa, conforme legislação pertinente.

Fica estabelecido que não há exigência de progressividade de penalidades para a configuração da justa causa. Assim, a Diretoria do CRCPR, no exercício do poder diretivo e disciplinar que lhe compete, poderá aplicar diretamente a penalidade quando caracterizada falta grave, de forma proporcional e devidamente fundamentada.

Documento substitui a versão de 11/04/2022 – Deliberação 028/2022