DELIBERAÇÃO CRCPR Nº 028/2022, DE 11 DE ABRIL DE 2022
(Ata 1.374ª)

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

O Plenário do **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,

DELIBERA, no sentido de:

Art. 1º - Aprovar a Política de Segurança de Informação do Conselho Regional de Contabilidade do Paraná.

Art. 2º - Esta Deliberação entra em vigor na data de sua assinatura, revogando-se as disposições em contrário.

ORIGINAL ASSINADO
Contador **LAUDELINO JOCHEM**
Presidente
CO – CRCPR Nº 44.143/O

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A política de segurança da informação deve adotar critérios técnicos e administrativos aptos a proteger os dados pessoais de acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, ou qualquer forma de tratamento inadequado, conforme previsão do art. 46 da Lei nº 13.709/2018 (LGPD). Para tanto, a entidade deve implementar soluções de natureza multidisciplinar, com observância do descrito na ISO 27001, visando a melhor segurança dos dados pessoais de pessoas naturais.

Assim, para assegurar os altos padrões de qualidade na prestação de serviços, faz-se necessária a especificação de uma política de segurança.

A finalidade dessa Política é descrever as normas de utilização e atividades que entendemos como violação ao uso dos serviços e recursos,os quais são considerados proibidos.

Podemos definir como serviços e recursos os equipamentos utilizados pelos colaboradores tais como: computadores, impressoras, e-mails do domínio crcpr.org.br, link de internet e afins.

As normas descritas no decorrer deste documento não constituem uma relação exaustiva e podem ser atualizadas com o tempo, sendo que qualquer modificação será avisada em tempo hábil para remodelação (se necessário)do ambiente.

Tais normas são fornecidas a título de orientação do colaborador. Em caso de dúvida sobre o que é considerado, de alguma forma, violação, o usuário deverá enviar previamente um e-mail para informatica@crcpr.org.br visando esclarecimentos e segurança.

Caso seja necessário advertir o colaborador, será informado ao Recursos Humanos para interagir e manter-se informado da situação.

As políticas de segurança foram divididas em oito tópicos, que são:

1. **Utilização da informação e recursos**
2. **Utilização da Rede**
3. **Computação pessoal e móvel**
4. **Políticas de Senhas**
5. **Gestão da Identidade**
6. **Utilização de E-Mail**
7. **Utilização de acesso à Internet**
8. **Utilização de impressoras**
9. **Manuseio e armazenamento de documentação física**
10. **Verificação da utilização da Política de Utilização da Rede**
11. **Cadastro do ponto eletrônico**
12. **Do tratamento de dados de colaboradores**
13. **Das Punições**

A seguir descreveremos as normas mencionadas e informamos que tudo o que não for permitido e/ou liberado é considerado violação à Política da Utilização da Rede.

1. UTILIZAÇÃO DAS INFORMAÇÕES E RECURSOS

A liberação de acesso às informações para os usuários será autorizada através do Controle de Usuários e, levará em consideração a necessidade de utilização por cada colaborador, observando-se o grau de sigilo das informações.

O acesso aos dados pessoais deverá ser autorizado apenas para usuários que necessitam dos mesmos para desempenho de suas atividades profissionais no CRCPR. Cada usuário deverá tratar apenas as informações e ambientes previamente permitidos. A tentativa consciente de acesso a ambientes/dados não autorizados será passível de punição.

O acesso das informações armazenadas e processadas em ambiente virtual é individual e intransferível. O acesso acontecerá mediante identificação e autenticação do usuário, devendo ser mantidos em segredo.

Os recursos de tecnologia fornecidos pela empresa são para uso exclusivo para realização das atividades profissionais. A utilização para fins pessoais é vedada. Em caso de necessidade de uso para fins pessoais, a gerência deve conceder permissão, com descrição do motivo, data e tempo de uso (em horas), com comunicação imediata à equipe de TI, para o devido monitoramento.

2. UTILIZAÇÃO DA REDE

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) Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta (também conhecido como “cracking”). Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes;

b) Não são permitidas tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques do tipo “negativa de acesso”, provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de “quebrar” (invadir) um servidor;

c) Não é permitido o uso de qualquer tipo de programa ou comando designado a interferir com sessão de usuários;

d) Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas acessados, evitando, desta maneira, o acesso por pessoas não autorizadas e se possível efetuar o logout/ logoff da rede ou bloqueio do desktop através de senha, bem como todos os computadores do CRCPR serão configurados para bloqueio automático após cinco minutos em desuso.

e) Falta de manutenção no diretório pessoal, evitando acúmulo de arquivos inúteis;

f) Material de natureza pornográfica e racista não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede;

g) Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas. As áreas de armazenamento de arquivos são designadas conforme 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 alguns casos pode haver mais de um compartilhamentoreferente aos arquivos do departamento em qual faz parte.

h) A pasta GERAL ou similar, não deverá ser utilizada para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza sensível;

i) É obrigatório armazenar os arquivos inerentes o CRCPR no servidor de arquivos para garantir o backup dos mesmos, não é realizado backup nos arquivos do OneDrive;

j) Haverá limpeza semanal dos arquivos armazenados na pasta GERALou similar, para que não haja acúmulo desnecessário de arquivos;

k) É proibida a instalação ou remoção de softwares que não forem devidamente acompanhadas pela Divisão de Informática, todas as solicitações deverão ser feitas através de e-mail;

l) É vedada a abertura de computadores para qualquer tipo de reparo, caso seja necessário o reparo deverá ocorrer pela Divisão de Informática;

m) Não será permitida a alteração das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro;

n) É vedada a instalação de softwares e hardwares sem autorização/auxílio da equipe técnica.

o) É vedada a realização de downloads de filmes, músicas, fotos em sites de pirataria, os quais são monitorados pela equipe de TI.

p) É vedada a utilização de dispositivos pessoais de memória externa. Em caso de necessidade, os mesmos deverão ser fornecidos pela equipe de TI.

q) É vedada a utilização de aplicativos de mensagens instantâneas (Whatsapp Web, Skype), em contas pessoais, nas estações de trabalho, exceto a equipe de gestores que disponibiliza o smartphone pessoal para uso profissional.

r) As portas USB dos computadores se encontram bloqueadas. Em caso de necessidade de utilização, deverá haver autorização formal da chefia, com

comunicação à equipe de TI para liberação. Os smartphones não devem ser carregados nas estações de trabalho. Em caso de necessidade, realize o carregamento na tomada elétrica.

s) Em caso de necessidade de utilização de sites de transferência de arquivos, em razão do tamanho do documento, deverá ser utilizada conta própria no OneDrive (Office 365), a ser fornecida pela equipe de TI.

3. COMPUTAÇÃO PESSOAL E MÓVEL

Os dados pessoais existentes nos sistemas do CRCPR somente serão utilizados em recursos do próprio CRCPR. É proibido o uso de equipamentos pessoais para tratamento de dados pessoais ou para manuseio se sistemas corporativos, salvo mediante autorização da gerência e comunicação ao setor de TI.

As estações de trabalho são pessoais e, portanto, configuradas com as permissões necessárias para a prestação de serviços de cada colaborador. A necessidade de utilização de estação de trabalho de outro colaborador deve ser devidamente autorizada pela chefia, mediante comunicação imediata à equipe de TI, com indicação do motivo, data e tempo de uso (em horas);

É obrigatório o bloqueio das estações de trabalho durante a ausência do colaborador.

4. POLÍTICA DE SENHAS

Senhas são um meio comum de validação da identidade do usuário para obtenção de acesso a um sistema de informação ou serviço. Convém que a concessão de senhas seja controlada, considerando: as senhas temporárias devem ser alteradas imediatamente, não devem ser armazenadas de forma desprotegida, entre outros.

a) A senha deverá ser redefinida a cada 42 (quarenta e dois) dias;
b) As responsabilidades do usuário incluem, principalmente, os cuidados para a manutenção da segurança dos recursos, tais como sigilo da senha e o monitoramento de sua conta, evitando sua utilização indevida. As senhas são sigilosas, individuais e intransferíveis, não podendo ser divulgadas em nenhuma hipótese;
c) Tudo que for executado com a senha de usuário da rede ou de outro sistema será de inteira responsabilidade do usuário, por isso, tome todo o cuidado e mantenha sua senha secreta;
d) As senhas são efetivas apenas quando usadas corretamente, requer cuidados na sua escolha e uso, alguns deles estão descritos abaixo:

- Não utilize informações pessoais fáceis de serem obtidas, como o número de telefone, nome da rua, nome do bairro, cidade, data de nascimento, etc;
- Utilize senha com, pelo menos, sete caracteres;
- Misture caracteres maiúsculos e minúsculos;

- Misture números, letras e caracteres especiais;
- Inclua, pelo menos, um caractere especial.

5. GESTÃO DE IDENTIDADES

A política de gestão de identidades visa a estabelecer os limites e permissões de acesso a dados pessoais que para cada funcionário, de acordo com seu respectivo cargo. Para tanto:

Gerente Operacional e Equipe de TI: terá acesso a todos os dados pessoais do banco de dados da empresa.

Gerente e coordenador: terá acesso a todos os dados pessoais referentes ao seu setor.

Em caso de troca de setor ou de cargo, as permissões de acesso serão revisadas, podendo ser revogadas se o funcionário não desempenhar atividades que as utilizem.

Controle de Acessos

Os colaboradores receberão acesso aos sistemas, conforme a necessidade de acesso prevista na descrição do cargo e da Divisão, com utilização de usuário e senhas.

6. UTILIZAÇÃO DE E-MAIL

Esse tópico visa definir as normas de utilização de e-mail que engloba desde o envio, recebimento e gerenciamento das contas de e-mail.

A conta de e-mail é disponibilizada exclusivamente para uso institucional não sendo admitido para uso pessoal.

Todos os usuários de e-mail devem tomar ciência que a Internet opera em domínio público que foge do controle da equipe técnica desta Instituição. As mensagens podem estar sujeitas a demora e serviços potencialmente não confiáveis.

Grande parte da comunicação do dia a dia passa através de e-mails. Mas é importante também lembrar que grande parte das pragas eletrônicas atuais chega por esse meio. Os vírus atuais são mandados automaticamente, isso significa que um e-mail de um profissional, colega ou amigo não foi mandado necessariamente pelo mesmo.

Nosso servidor de e-mail encontra-se protegido contra vírus e códigos maliciosos, mas algumas atitudes do usuário final são importantes. Para isto é importante que algumas regras sejam obedecidas.

a) O e-mail deve ser utilizado de forma consciente, evitando qualquer tipo de perturbação a outras pessoas, seja através da linguagem utilizada, frequência ou tamanho das mensagens;
b) O envio de e-mail deve ser efetuado somente para pessoas que desejam recebê-

los, se for solicitada a interrupção do envio a solicitação deve ser acatada e o envio não deverá acontecer;

c) É proibido o envio de grande quantidade de mensagens de e-mail (spam) que, de acordo com a capacidade técnica da Rede, seja prejudicial ou gere reclamações de outros usuários. Isso inclui qualquer tipo de mala direta, como, por exemplo, publicidade, comercial ou não, anúncios e informativos, ou propaganda política;

d) É proibido reenviar ou de qualquer forma propagar mensagens em cadeia independentemente da vontade do destinatário de receber tais mensagens;

e) É proibido enviar fotos de documentos ou informações do CRCPR através de mídias do celular. Em caso de recebimento, o colaborador deverá transmiti-lo imediatamente para seu computador corporativo, excluindo a mídia terminantemente de seu dispositivo móvel.

f) Os documentos e informações deverão ser transmitidos exclusivamente através do e-mail corporativo e da ferramenta de comunicação interna **SPARK ou Microsoft Teams.**

g) Evite mandar e-mail para mais de 10 (dez) pessoas de uma única vez, é proibido o envio de e-mail mal-intencionado, tais como mail bombing ou sobrecarregar um usuário, site ou servidor com e-mailmuito extenso ou numerosas partes de e-mail;

h) Caso o CRCPR julgue necessário haverá bloqueios:

   a. De e-mail com arquivos anexos que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;

   b. De e-mail para destinatários ou domínios que comprometa o usode banda ou perturbe o bom andamento dos trabalhos;

i) É proibido forjar qualquer das informações do cabeçalho doremetente;

j) Não é permitida má utilização da linguagem em respostas aose-mails comerciais, como abreviações de palavras ou uso de gírias;

k) É obrigatória a manutenção da caixa de e-mail, evitando acúmulode e-mails e arquivos inúteis;

l) Para certificar-se que a mensagem foi recebida pelo destinatário, deve-se, se necessário, utilizar procedimentos de controle extras para verificar a chegada da mensagem, e solicitar notificações de “recebimento” e “leitura”;

m) Não execute ou abra arquivos anexados enviados por emitentesdesconhecidos ou suspeitos;

n) Não abra arquivos anexados com as extensões .bat, .exe, .src, .lnk e .com se não tiver certeza absoluta que solicitou este e-mail;

o) Desconfie de todos os e-mails com assuntos estranhos e/ou em inglês. Alguns dos vírus mais terríveis dos últimos anos tinham assuntos como: ILOVEYOU, Branca de neve pornô, etc;

p) Preferencialmente a utilização de assinatura nos e-mails com o seguinte formato ou imagem abaixo (Padronizada pela diretoriadesta casa):

Nome do FuncionárioFunção

Telefone Comercial

CRCPR
CONSELHO REGIONAL DE CONTABILIDADE DO PARANÁ

Nome
Cargo
(41) 3360-4700
www.crcpr.org.br | facebook.com/CRCPR | @crc_parana

Imagem Exemplo

q) O CRCPR possui um sistema de Anti-Spam onde o próprio usuário pode administrar os e-mails que considera como spam, basta acessar o site http://antispam.crcpr.org.br (qualquer dúvida entre em contato com a Divisão de Informática)

r) Abaixo algumas regras para melhorar a comunicação nos e-mails:

- **Use Corretamente os campos de destinatários (Para, Cc, 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

- **Use o termo "Ação:" no início do Assunto ao requisitar uma ação**

  Ex.: "Ação: realizar empenho da empresa XYZ. Prazo 7/julho."

- **Estruture o conteúdo do e-mail em 3 partes**

  Objetivo: breve resumo do objetivo, para criar o contexto damensagem.

  Ação requerida e prazo: informar claramente, se possível emdestaque.

  Histórico e informações adicionais: devem vir no final,

  preferencialmente em anexos se for muita informação.

- **Evite parágrafos longos, e-mails extensos e planos de cores que dificultem a leitura**

- **Evite utilizar letras maiúsculas no corpo do e-mail:** Um e-mail exclusivamente composto de letras maiúsculas é muitas vezes vistocomo rude ou como se estivesse "gritando" com o destinatário, por isso, utilize-as apenas no início das frases ou quando quiser darênfase a uma palavra particular

- **Evite enviar arquivos anexos grandes**

- **A responder um e-mail não use "Responder a todos"!**

  Evite ao máximo Responder a Todos em e-mails com mais de 5pessoas

- **Antes de enviar um e-mail faça um checklist dos campos principais (destinatários, assunto, conteúdo)**

  Certifique-se que: todos os destinatários precisam receber amensagem;

O campo assunto inicia com “Ação:” (quando houver uma ação);O conteúdo da mensagem está claro e o formato esta adequado.

7. UTILIZAÇÃO DE ACESSO À INTERNET

Esse tópico visa definir as normas de utilização da Internet queenglobam desde a navegação a sites, downloads e uploads de arquivos.

A Internet é uma ferramenta de trabalho e deve ser usada para estefim pelos colaboradores.

A Divisão de Informática poderá bloquear acesso à sites sempreque comprometer o fluxo de dados de áreas críticas.

a) É proibido utilizar os recursos do CRCPR para fazer o download ou distribuição de software ou dados não legalizados;
b) É proibida a divulgação de informações confidenciais do CRCPR em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei;
c) Poderá ser utilizada a Internet para atividades não relacionadas comos serviços durante o horário de almoço, ou fora do expediente, desde que dentro das regras de uso definidas nesta política;
d) Os colaboradores com acesso à Internet podem baixar somente programas ligados diretamente às atividades do CRCPR e devem providenciar o que for necessário para regularizar a licença e o registro desses programas;
e) Colaboradores com acesso à Internet não podem efetuar upload de qualquer software licenciado ao CRCPR ou de dados de propriedade da CRCPR, sem expressa autorização da Divisão de Informática;
f) Caso o CRCPR julgue necessário haverá bloqueios de acesso a:
    a. Arquivos que comprometam o uso de banda ou perturbe o bom andamento dos trabalhos;
    b. Domínios que comprometam o uso de banda ou perturbem o bom andamento dos trabalhos;
g) Haverá geração de relatórios dos sites acessados por usuário e se necessário a publicação desse relatório;
h) É obrigatória a utilização do(s) software(s) homologado(s) pelo Setor de Informática tais como Mozilla FireFox, Internet Explorer, Google Chome como cliente(s) de navegação;

i) Não serão permitidos softwares de comunicação instantânea, tais como Skype, Yahoo Messenger, Facebook Messenger e afins, parafins particulares;
j) Não será permitida a utilização de softwares de peer-to-peer (P2P), tais como Kazaa, Morpheus, BitTorrent e afins;
k) Não será permitido o acesso a sites de relacionamentos tipo Facebook, Orkut, Gazag, etc,;
l) O acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas, é bloqueado e as tentativas de acesso serão monitoradas;
m) Não será permitida a utilização de serviços de streaming, tais comoRádios On-Line e afins.

8. UTILIZAÇÃO DE IMPRESSORAS

Esse tópico visa definir as normas de utilização de impressoras disponíveis na rede interna.

a) Antes de mandar imprimir, deve-se verificar se a impressora está ligada e abastecida de papel e, quando esta estiver ligada a um computador, se o mesmo também está ligado;

b) Se a impressão deu errada e o papel pode ser reaproveitado na sua próxima tentativa, recoloque-o na bandeja de impressão. Se o papel servir para rascunho, leve para sua mesa. Se o papel não servir para mais nada, jogue no lixo;

c) Não é permitido deixar impressões erradas na mesa das impressoras, na mesa das pessoas próximas a ela e tampouco sobre o gaveteiro;

d) Se a impressora emitir alguma folha em branco recoloque-a na bandeja;

e) Se você notar que o papel de alguma das impressoras está no final, faça a gentileza de reabastecê-la. Isso evita que você e outras pessoas tenham seus pedidos de impressão prejudicados e evita acúmulo de trabalhos na fila de impressão;

f) Utilize a impressora colorida somente para versão final de trabalhos e não para testes ou rascunhos;

g) Sempre que possível utilize a impressão em frente e verso, para um melhor aproveitamento do papel.

9. MANUSEIO E ARMAZENAMENTO DE DOCUMENTAÇÃO FÍSICA

Todos os procedimentos que possibilitam a proteção da informação e a continuidade do seu uso devem ser documentados, de tal forma que possibilite a operacionalização desses procedimentos, mesmo na ausência do usuário responsável.

Os documentos em meio analógico, que contenham dados pessoais ou dados pessoais sensíveis, devem ser guardados em envelopes/pastas e armazenados em gavetas ou armários.

Não deixe documentos que contenham dados pessoais sobre sua mesa.

Imprima somente o necessário.

Selecione as folhas que serão utilizadas para rascunho e descarte as que contenham informações confidenciais, com utilização do triturador de papel.

Os documentos que contenham dados pessoais devem ser armazenados em locais com chave, com acesso restrito, formalizado através de termo entre a gestão e o funcionário que tiver a entrada franqueada.

Os documentos arquivados terão regramento específico com base na Classificação Documental e Tabela de Temporalidade.

10. VERIFICAÇÃO DA UTILIZAÇÃO DA POLÍTICA DE UTILIZAÇÃO DA REDE

Para garantir as regras mencionadas acima o CRCPR se reserva nodireito de:

a) Implantar softwares e sistemas que podem monitorar e gravar todos os usos de Internet através da rede e das estações de trabalhodo CRCPR;

b) Inspecionar qualquer arquivo armazenado na rede estejam no disco local da estação ou nas áreas privadas da rede, visando assegurar orígido cumprimento desta política;

c) Foram instalados uma série de softwares e hardwares para proteger a rede interna e garantir a integridade dos dados e programas, incluindo um firewall, que é a primeira, mas não a única barreira entre a rede interna e a Internet;

11. CADASTRO DO PONTO ELETRÔNICO

Em atenção à Portaria nº 1510/2009 do Ministério do Trabalho e Emprego, é necessária a utilização de registro de ponto eletrônico.

Na contratação do funcionário em regime de CLT, será realizado o cadastramento eletrônico no sistema desenvolvido pela equipe de TI do CRCPR, que poderá ser acessado via https://rh.crcpr.org.br/

12. DO TRATAMENTO DE DADOS DOS COLABORADORES

Dos nossos colaboradores e dependentes tratamos os dados pessoais listados para:

DADOS PESSOAIS	FINALIDADE	BASE LEGAL
Nome completo, inclusive o nome social	Contabilidade do Conselho, pagamento da folha de funcionários, devolução de valores pagos em duplicidade, registro e administração de funcionários, cadastro	Art. 7º, inciso II, III, V, VI da Lei nº 13.709/2018 (LGPD).
Data de nascimento e idade		
Nome dos genitores (pai e mãe)		
Estado civil		
Gênero		

Nível de instrução ou de escolaridade	no e-social, cadastro no INSS, cadastro no plano de saúde, repasse de informações ao Ministério do Trabalho. Utilizar os dados nas situações conjugais que podem ter reflexos em providências do CRCPR, como o pagamento de pensão, a inclusão de um dependente nos planos assistenciais. Utilizar os dados para fins de concessão de benefícios assistenciais e sociais (vale transporte, vale alimentação e vale refeição e plano de saúde).	
Endereço residencial completo		
Telefone (celular e fixo) e WhatsApp		
Endereços de correios eletrônico		
Certidão de nascimento, se for solteiro		
Certidão de casamento ou declaração de união estável		
Carteira de identidade (RG)		
Cadastro de pessoa física (CPF)		
Carteira nacional de habitação (CNH)		
Título de eleitor		
Certificado de Reservista		
Carteira de Trabalho e Previdência Social (física ou digital)		
Número e imagem do cartão de vale transporte (quando utilizado pelo (a) empregado (a)		
Número do Programa de Integração Social (PIS)		
Imagem do diploma de escolaridade		
Imagem de certificados de cursos e eventos		
Informações sobre o seu cargo, renda e classificação salarial no CRCPR		
Dados bancários (como banco, agência e número de contas correntes0		
Nome de usuário e senha específicos para uso dos serviços da controladora		
Término do contrato de trabalho, abrangendo o motivo do desligamento.		

Resultado do processo de avaliação de desempenho.		
DADOS PESSOAIS DE CRIANÇA E DE ADOLESCENTE	**FINALIDADE**	**BASE LEGAL**
Certidão de nascimento dos filhos menores de 14 anos.	Utilizar os dados nas situações conjugais que podem ter reflexos em providências do CRCPR, como o pagamento de pensão, a inclusão de um dependente nos planos assistenciais. Utilizar os dados para fins de concessão de benefícios assistenciais e sociais (vale transporte, vale alimentação e vale refeição e plano de saúde).	Art. 7º, inciso II, III, V, VI da Lei nº 13.709/2018 (LGPD).
Nome, data de nascimento, CPF dos dependentes para fins de imposto de renda.		
DADOS PESSOAIS SENSÍVEIS	**FINALIDADE**	**BASE LEGAL**
Fotografia	Para fins de identificação interna.	Art. 11º, inciso II alínea “a” e “g” da Lei nº 13.709/2018 (LGPD).
Exames e atestados médicos, especialmente admissionais periódicos e de retorno ao trabalho após afastamento superior a 30 dias em caso de doença, acidente ou parto, de mudança de função, demissionais e ainda aqueles que atestem doença ou acidente.	Cumprir com as exigências legais relativas à saúde do trabalhador, com vistas à realização de exames médicos admissional, periódico, complementar e demissional.	Art. 11º, inciso II alínea “a” e “d” da Lei nº 13.709/2018 (LGPD).

	Cumprir com as exigências relativas à segurança e medicina do trabalho. Executar programas de qualidade de vida.	
Filiação sindical	Para os respectivos descontos de contribuições sindicais;	Art. 11, inciso II, alíneas “a”
Origem racial ou étnica	Política de quotas	Art. 11, inciso II, alíneas “b”
DADOS PESSOAIS SENSÍVEIS DE CRIANÇA E DE ADOLESCENTE	**FINALIDADE**	**BASE LEGAL**
Atestado médico de dependente de funcionário Comprovante de comparecimento em consulta médica de dependente de funcionário Relação de consultas médicas comparecidas de dependente de funcionário Relação de consultas médicas realizadas por dependente de funcionário	Utilizar os dados nas situações conjugais que podem ter reflexos em providências do CRCPR, como o pagamento de pensão, a inclusão de um dependente nos planos assistenciais. Utilizar os dados para fins de concessão de benefícios assistenciais e sociais (vale transporte, vale alimentação e vale refeição e plano de saúde).	Art. 11º, inciso II alínea “a” e “d” da Lei nº 13.709/2018 (LGPD).

13. DAS PUNIÇÕES

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

a) Comunicação de descumprimento:

a. Será encaminhado ao funcionário, por e-mail, comunicado informando o descumprimento da norma, com a indicação precisada violação praticada.

b. Cópia desse comunicado permanecerá arquivada junto a Divisão de Recursos Humanos na respectiva pasta funcional do infrator.

b) Advertência ou suspensão:

a. 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. Nas hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, alíneas ¨a¨ à ¨f¨.

Por tratar-se o CRCPR de autarquia federal criada pelo Decreto-lei nº 9.295/96, os casos passíveis de aplicação de penalidades observarão o devido Processo Administrativo Disciplinar, para o qual será formada comissão específica.

Fica desde já estabelecido que não há progressividade como requisito para a configuração da dispensa por justa causa, podendo a Diretoria deste CRCPR, no uso do poder diretivo e disciplinar que lhe é atribuído, aplicar a pena que entender proporcionalmente devida quando tipificada a falta grave.