Política de Segurança da Informação - PSI CRF-RJ

O CRF-RJ

R E S O L V E

Estabelecer a Política de Segurança da Informação, no âmbito do Conselho Regional de Farmácia do estado do Rio de Janeiro

Prover orientação,

Esta política fornece orientação direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes (ref. NBR27002:2013) e regras para a promoção do uso adequado e responsável dos recursos do CRF-RJ, com o intuito de prover meios para proteger os usuários da rede local de ações ilegais ou danos que possam ser perpetrados por pessoas, internas ou externas a organização, sejam estas ações intencionais ou acidentais.

As orientações e regras aqui contidas são estabelecidas para prover meios de proteger tanto os funcionários, clientes, parceiros, especialistas, funcionários contratados em regime temporário, incluindo pessoal integrante de empresas contratadas e os próprios recursos da rede do CRF-RJ. Prestando aos funcionários serviços de rede de alta qualidade e ao mesmo tempo desenvolver um comportamento extremamente ético e profissional.

Assegurar que toda a informação, coletada, gerada, adquirida, utilizada, em trânsito e armazenada; própria, pessoal ou custodiada; por meio de tecnologias, procedimentos, pessoas e ambientes do CRF-RJ, deve ser tratada como parte do seu patrimônio e deve ser protegida quanto aos aspectos de confidencialidade, integridade e disponibilidade, bem como de proteção de dados pessoais, privacidade e conformidade legal.

As normas descritas no decorrer 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.

Assegurar que essas diretrizes sejam aplicáveis aos ambientes, sistemas, pessoas e processos do CRF-RJ , tanto no meio digital quanto nos meios analógicos de processamento, comunicação e armazenamento de informações.

1- Proteger conforme riscos

Estabelecer medidas de segurança pelo valor do ativo e em função dos riscos de impacto nos negócios, atividades e objetivos institucionais do CRF-RJ , com vistas à proteção de dados pessoais, à

privacidade e à conformidade legal, considerando o balanceamento de aspectos como tecnologias, austeridade nos gastos, qualidade e velocidade.

2 - Responsabilizar proprietário dos ativos

Considerar o funcionário, o conselheiro ou terceirizado, , proprietário dos ativos de informação sob sua responsabilidade, bem como responsável pela liberação e cancelamento do acesso, classificação de segurança e medidas de proteção de informação e dados.

3. Restringir acesso e uso de ativos

Assegurar que o acesso e o uso dos ativos sejam controlados e limitados às atribuições necessárias para cumprimento das atividades de funcionários, conselheiros e terceirizados autorizados e utilizados no estrito interesse do CRF-RJ , apenas para as finalidades profissionais, lícitas, éticas, administrativamente aprovadas e devidamente autorizadas. Qualquer outra forma de acesso e uso necessitará de prévia autorização do proprietário do ativo de informação.

4- Usar ativos seguros

Permitir somente o uso de ativos homologados e autorizados pelo CRF-RJ , capacidade, manutenção e contingência adequadas e sua operação deve estar de acordo com a legislação, e desde que sejam identificados de forma individual, inventariados, protegidos e tenham um proprietário responsável. Os ativos devem ter documentação atualizada, riscos mapeados, a Política de Segurança da Informação do ente, cláusulas contratuais e legislação em vigor.

5. Tratar informações e dados conforme classificação

Tratar as informações e dados segundo sua classificação de segurança, aposta de maneira a serem adequadamente protegidos quando da sua coleta, criação, utilização, custódia e descarte, para assegurar sua confidencialidade, integridade, disponibilidade.

6 Assegurar a proteção de dados pessoais e a privacidade

Proteger dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito que possa afetar a privacidade do titular (ref. Lei Federal 13709/2018).

7. Manter segurança nos serviços em nuvem

Assegurar que toda a cadeia de suprimentos de TI baseada em provedores de serviços no ambiente de computação em nuvem seja avaliada por todos os aspectos da segurança, incluindo o cumprimento da

legislação e regulamentação local e global, o gerenciamento de identidades, o monitoramento e auditoria regulares e as restrições de localização geográfica para proteger dados, metadados, informações e conhecimentos produzidos ou custodiados pelo CRF-RJ.

8. Dar continuidade de uso dos serviços críticos

Assegurar a disponibilidade, o uso, o acesso e a proteção dos ativos que suportam os serviços e processos críticos do CRF RJ , por intermédio de ações de administração de crise, prevenção e recuperação, estabelecendo uma estratégia de continuidade de negócio para reduzir a um nível aceitável a possibilidade de interrupção causada por desastres ou falhas.

9. Monitorar e auditar permanentemente

Monitorar e auditar periodicamente o cumprimento da Política de Segurança da Informação, pelas áreas competentes, respeitando-se os princípios legais e normativos.

10. Conscientizar de forma contínua

Assegurar que funcionários, conselheiros e terceirizados sejam continuamente capacitados e conscientizados sobre os procedimentos de proteção e uso correto dos ativos do CRF-RJ quando da realização de suas atividades, bem como estejam conscientes e cumpram suas responsabilidades, de forma a minimizar riscos.

11. Notificar via canal único

Notificar a área responsável por tratamento incidentes caso o funcionário, conselheiro ou terceirizado identifique qualquer quebra ou fragilidade na segurança da informação.

12.Comunicar no âmbito interno e externo

Recomendar que diretrizes, normas e procedimentos da política de segurança da informação sejam definidos, aprovados pela Direção, publicados e comunicados para todos os funcionários, conselheiros e terceirizados e partes externas relevantes (ref. NBR27002:2013).

13.ANÁLISE CRÍTICA DAS ESPÉCIES NORMATIVAS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Cada espécie normativa da Política de Segurança da Informação – diretrizes, normas e procedimentos - deve ser revista em intervalos planejados, não superiores a 2 (dois) anos, a partir de sua data de publicação, ou em caso de condições obrigatórias de atualização do documento, como:

I - Edição ou alteração de leis e/ou regulamentos;

II - Mudança estratégica da instituição;

III - Expiração da data de validade do documento;

IV - Mudanças de tecnologia na organização; ou

V - A partir dos resultados das análises de risco que estabeleçam a necessidade de mudança da norma para readequação da instituição aos riscos (mitigação).

Competirá ao Serviço de Tecnologia da Informação o monitoramento de periódico das normas, bem como sua complementação por intermédio dos demais instrumentos que compõem a Política de Segurança da Informação CRF-RJ. A aprovação das alterações nas normas que compõe a Política de Segurança da Informação competirá aos gestores do CRF-RJ. O risco de análise crítica para determinar a adequação, suficiência e eficácia das normas deve ser suportado por procedimento formal com registro das sugestões de melhorias e das decisões tomadas em documento específico.

Referências

Normas Tecnicas ABNT NBR ISO/IEC 27002:2013 — Tecnologia da Informação — Técnicas de Segurança — Código de Prática para controles de segurança da informação.

Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

I - Utilização dos Recursos Computacionais

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

1. Recursos computacionais - São os equipamentos, as instalações ou bancos de dados direta ou indiretamente administrados, mantidos ou operados *pelo* CRF-RJ, tais como:

- Computadores e terminais de qualquer espécie, incluídos seus equipamentos acessórios;
- Impressoras;
- Redes de computadores e de transmissão de dados;
- "Arrays" de discos, de fitas, de "juke boxes" e equipamentos afins;
- Bancos de dados ou documentos residentes em disco, fita ou outros meios;
- Leitoras de códigos de barra, "scanners", equipamentos digitalizadores e afins;
- Manuais técnicos;
- Salas de computadores;
- Serviços e informações disponibilizados via a arquitetura de informática da instituição

- Softwares adquiridos.

2. Mobiliário e Material de Consumo - São as cadeiras, mesas e demais móveis relacionados ao uso de computadores e terminais e os materiais de consumo, tais como: discos, disquetes, "compact disc", formulários, papéis, toner para impressora, etc.

3. Privacidade - O CRF-RJ tem direito de acesso a qualquer informação salva em formato eletrônico em seus equipamentos de rede ou "nuvem", que se encontrem fisicamente no mobiliário do escritório, como, por exemplo, em mesas, estantes, gaveteiros, armários etc. Dessa forma, ainda que o Colaborador possa se utilizar da estrutura de tecnologia da organização para algum uso particular não conflitante, tais informações podem ser acessadas pela CRF-RJ mesmo sem o prévio consentimento do respectivo Colaborador.

Com relação às ligações telefônicas, e-mails e outros canais de comunicação internos, a CRF-RJ se reserva o direito de monitorar e armazenar registros das ligações e conversas de texto, bem como consultá-las sem prévio aviso ao Colaborador.

Sem prejuízo do acima exposto, a CRF-RJ garante que toda escuta a conversas telefônicas e mensagens de texto depende do prévio consentimento da Diretoria de *Compliance*. Mais ainda, a CRF-RJ se compromete a zelar pelo sigilo de qualquer informação, incluindo de caráter pessoal, que eventualmente se depare nos processos de monitoramento.

4 - Proteção do Patrimônio Físico e Intangível

Integram o patrimônio físico e intangível da CRF-RJ, seus imóveis, instalações, veículos, equipamentos, estoques, valores, planos, produtos, tecnologia, estratégia de negócio e de comercialização, informações, pesquisas e dados que devem ser protegidos pelos funcionários, não podendo os mesmos serem utilizados para obtenção de vantagens pessoais e nem fornecidos a terceiros, independentemente do fim.

Não podem ser utilizados equipamentos ou outros recursos da CRF-RJ para fins particulares, salvo se previamente autorizado pelo gestor de área, sendo a referida aprovação vetada nos casos em que interfira no seu trabalho, ou se ainda:

(i) Interferir ou concorrer com os negócios da CRF-RJ;

(ii) Fornecer informações a terceiros;

(iii) Envolver solicitação comercial ou outra solicitação não apropriada ao negócio, e;

(iv) Envolver custo adicional para a CRF-RJ.

5. O usuário deverá informar imediatamente à área de informática e ao responsável imediato em caso de ocorrência de vírus

6. É proibido alimentar-se e fumar próximo aos equipamentos de informática;

Não serão permitidos:

1 Tentativas deliberadas para interferir em um serviço, sobrecarregar um serviço ou, ainda, tentar desativar um host, inclusive aderir a ataques de negação de serviços.

2 Usar programa/script/comando ou enviar mensagem de qualquer espécie com a intenção de interferir ou desabilitar uma sessão de terminal de usuário, via qualquer meio, localmente ou remoto.

3 Passar qualquer tipo de informação a terceiros sobre a estrutura física e lógica da rede corporativa.

4 Introduzir programas com códigos maliciosos na rede ou servidores (exemplo: vírus, worms, cavalos de tróia, e-mail bombing).

5 Revelar códigos de identificação, autenticação e autorização de uso pessoal (conta, senhas) ou permitir o uso por terceiros de recursos autorizados por meio desses códigos. Isso inclui membros da família, quando o trabalho estiver sendo realizado em sua residência.

6 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 seu computador através de senha;

7 Instalar, distribuir ou utilizar softwares "pirateados" ou não licenciados para uso na rede corporativa do CRF-RJ;

8 Criar, transmitir, distribuir, colocar, armazenar ou tornar disponível através do CRF-RJ e da Internet qualquer material que viole leis ou regulamentações referentes a obscenidade, indecência, ou pornografia infantil; material que divulgue informações injuriosas, caluniosas ou difamatórias, que viole o direito à honra ou à imagem das pessoas; material que constitua ameaça a alguém ou qualquer material que viole quaisquer leis e regulamentações vigentes.

9 Fazer cópia não autorizada de material protegido por direitos autorais, incluindo, mas não limitado a: músicas, textos, digitalização e distribuição de fotografias encontradas em revistas, livros ou em outras fontes protegidas por direitos autorais;

10 É obrigatório armazenar os arquivos inerentes a empresa no servidor de arquivos para garantir o backup dos mesmos;

11 É proibida a instalação ou remoção de softwares que não forem devidamente acompanhados pelo departamento técnico, através de solicitação escrita que será disponibilizada;

12 Usuários podem estar isentos dessas restrições durante o curso de suas responsabilidades legítimas (exemplo: administradores de recursos podem ter a necessidade de desativar o acesso a um equipamento se este estiver afetando negativamente os serviços do CRF-RJ.

13 A abertura de computadores para qualquer tipo de reparo, caso seja necessário o reparo deverá ocorrer pelo departamento técnico;

- Alteração de dados ou de equipamentos - os usuários, a menos que tenham uma autorização específica para esse fim, não podem tentar, permitir ou causar qualquer alteração ou destruição de ambientes operacionais, dados ou equipamentos de processamento ou comunicações instalados no CRF-RJ, de sua propriedade ou de qualquer outra pessoa. Essas alterações incluem, mas não se limitam, as alterações de dados, reconfiguração de chaves de controle ou parâmetros.

14 A alteração das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro.

15 Utilizar equipamento pessoal nas instalações do CRF-RJ.

II - Utilização de E-Mail

Esse tópico visa definir as normas de utilização do correio eletrônico que engloba desde o envio, recebimento e gerenciamento das contas de e-mail.
Responsabilidade pela conta - toda conta é de responsabilidade e de uso exclusivo de seu titular, não podendo esse permitir ou colaborar com o acesso aos recursos computacionais por parte de pessoas não autorizadas. Os usuários são responsáveis por qualquer atividade desenvolvida através de suas contas no CRF-RJ e pelos eventuais custos dela decorrentes em atividades não autorizadas;

O usuário é o único responsável pelo conteúdo das transmissões feitas através do e-mail a partir de sua conta e senha;

O uso da conta de e-mail corporativo do CRF-RJ é para fins profissionais, sendo permitido seu uso pessoal com bom-senso, para assuntos que não sejam conflitantes com as atividades do CRF-RJ nem que prejudiquem qualquer lei, regulação ou regulamento e políticas internas da CRF-RJ

Não serão permitidos:

1. Não é permitida a utilização dos recursos computacionais do CRF-RJ para benefício financeiro direto ou indireto, próprio ou de terceiros fora da empresa, sujeitando-se o infrator a imediata suspensão de sua conta.

2. O envio de e-mail a qualquer pessoa que não o deseje receber. Se o destinatário solicitar a interrupção de envio e-mails, o usuário deve acatar tal solicitação e não lhe enviar qualquer e-mail;

3. O envio de grande quantidade de mensagens de e-mail ("junk mail" ou "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;

4. Reenviar ou de qualquer forma propagar mensagens em cadeia ou "pirâmides", independentemente da vontade do destinatário de receber tais mensagens;

Caso o CRF-RJ julgue necessário haverá bloqueios:

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

- É proibido forjar qualquer das informações do cabeçalho do remetente;

- Não é permitida má utilização da linguagem em respostas aos e-mails comerciais, tais abreviações de palavras (Ex.: ¨vc¨ ao invés de ¨você¨);

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

- Obrigatoriedade da utilização do programa Outlook Express, ou outro software homologado pelo departamento técnico, para ser o cliente de e-mail;

É obrigatória a utilização de assinatura nos e-mails com o seguinte formato:

Nome do Funcionário
Função
Telefone Comercial
http://www.crf-rj.org.br

III. Utilização de acesso a Internet e da Intranet

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

Não serão permitidos:

1 Utilizar os recursos da empresa para fazer o download ou distribuição de software ou dados não legalizados;

2 Divulgar informações confidenciais da empresa 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;

3 Funcionários com acesso à Internet não podem efetuar upload de qualquer software licenciado à empresa ou de dados de propriedade da empresa ou de seus clientes, sem expressa autorização do gerente responsável pelo software ou pelos dados;

4 *Softwares de comunicação instantânea, tais como ICQ, Microsoft *Messenger* e afins;

5 A utilização de softwares de *peer-to-peer* (P2P), tais como *Kazaa* e afins;

6 A utilização de serviços de *streaming*, tais como Rádios On-Line e afins.

7 Não devem ser abertos arquivos ou executados programas anexados aos e-mails sem antes ter certeza de sua procedência e existência de prévia expectativa do recebimento da mensagem;

8 Dentro do aplicativo ou visualizador de e-mails, devem sempre estar desabilitadas as opções que permitam abrir ou executar automaticamente arquivos ou programas anexados às mensagens;

9 Não deve ser utilizado e-mail para fins ilegais;

10 Não devem ser transmitidos quaisquer materiais ilegais ou de qualquer forma censuráveis através deste serviço;

11 Não devem ser transmitidos quaisquer materiais que violem direitos de terceiros, incluindo, mas sem limitação, direitos de propriedade intelectual;

12 Não devem ser transmitidos quaisquer materiais que violem leis ou regulamentos locais, estaduais, nacionais ou internacionais aplicáveis;

13 O Colaborador não pode obter ou tentar obter acesso não-autorizado a outros sistemas ou redes de computadores conectados ao serviço;

14 Não devem ser utilizados os serviços de e-mail para transmitir quaisquer materiais que contenham vírus, arquivos do tipo "Cavalo de Tróia" ou outro programa prejudicial;

15 Não devem ser transmitidas mensagens não-solicitadas, conhecidas como *spam* ou *junkmail*, correntes, *chain letters* ou distribuição em massa de mensagens não-solicitadas, salvo mensagens informativas de produtos e serviços da CRF-RJ, aprovada por um Diretor, por lista controlada e via ferramentas oficiais contratas pela CRF-RJ. Quando este envio ocorrer, deve contar com sistema de cancelamento de cadastramento na própria mensagem;

16 Mensagens com assuntos confidenciais não devem ser impressas em impressoras usadas por outros usuários, sem que se esteja cuidando para retirar a impressão antes do acesso físico ao conteúdo impresso, de forma inadvertida, pelos demais usuários;

17 O e-mail deve estar ativo sempre que o usuário estiver trabalhando no microcomputador. Quando este se afastar de sua estação de trabalho, deve encerrar a sessão ou acionar recurso de proteção de tela com senha pessoal;

18 Não é permitido enviar músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura de rede local ou que violem as leis de direitos autorais

Caso o CRF-RJ julgue necessário haverá bloqueios de acesso à:

- Arquivos e domínios que comprometam o uso de banda ou perturbe o bom andamento dos trabalhos;

- Haverá geração de relatórios das localidades acessadas por usuário e se necessário a publicação desse relatório;

- Obrigatoriedade da utilização do programa Internet Explorer, ou outro software homologado pelo departamento técnico, para ser o cliente de navegação .

IV. Utilização das impressoras

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

1. Ao mandar imprimir, verifique na impressora se o que foi solicitado já está impresso. Há várias impressões "sem dono" acumulando-se;

2. Se a impressão deu errado 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.

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

4. Se a impressora emitir alguma folha em branco, recoloque-a na bandeja;

5. 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;

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

7. Quaisquer impressões, sobretudo as que contêm informações confidenciais, devem ser imediatamente retiradas da impressora;
8. Esta ferramenta deve ser utilizada apenas quando o documento físico se fizer imprescindível, evitando desperdícios ou gastos desnecessários;
9. As impressoras são ferramentas para fins profissionais, objetivando aumentar a produtividade nas atividades desenvolvidas pela CRF-RJ. Impressões para finalidade pessoal devem ser limitadas e com bom-senso, nunca com finalidades conflitantes com os interesses da CRF-RJ, bem como nunca infringindo nenhuma lei, norma, regulamentação e normas e políticas internas da CRF-RJ.

V- UTILIZAÇÃO DO TELEFONE

Seguem as regras que devem ser observadas por todos os Colaboradores quando da utilização destas ferramentas:

(i) O uso do telefone fixo na CRF-RJ deve ter uso para fins profissionais. É permitido o uso para fins pessoais com bom-senso, para assuntos que não sejam conflitantes com as atividadesda CRF-RJ nem que prejudiquem qualquer lei, regulação ou regulamento e políticas internas da CRF-RJ. Vale lembrar também que todas as ligações são gravadas e podem ser ouvidas pela CRF-RJ como determinam suas políticas.

(ii) O uso de telefone localizado fora das dependências da CRF-RJ para discussão de assuntos confidenciais internos pode ser necessário, principalmente em situações de contingência, porém pode gerar exposição de segurança, portanto, deve-se sempre priorizar fazer ligações dentro da CRF-RJ, ou pelos meios eletrônicos de telefonia e comunicação disponibilizados pela empresa via

computador e/ou aplicativos aprovados pela STI. Caso não seja possível, deve-se certificar que não existem terceiros ouvindo a ligação;

(iii) Não se deve deixar mensagens confidenciais em secretárias eletrônicas, pois essas podem ser resgatadas por pessoas não autorizadas, e;

(iv) Ao coordenar uma teleconferência ou videoconferência, deve-se garantir que todos os participantes foram devidamente autorizados antes de começar a reunião.

VI - Mesa Limpa

A política de mesa limpa consiste em não deixar informações confidenciais ou bens do CRF-RJ, incluindo, mas não se limitando a papéis, pen-drives ou quaisquer outros tipos de mídias removíveis, acessíveis a outras pessoas sem a devida proteção, quando o funcionário estiver fora de sua estação de trabalho.

Ao final do dia de trabalho, computadores portáteis devem ser devidamente trancados em gaveta ou armário, ou serem presos a cabos de segurança ou levados pelo seu responsável, conforme estabelecido pelo respectivo gestor.

VII - Tela Limpa

Computadores, notebooks e outros dispositivos devem estar protegidos por senha quando não estiverem sendo utilizados. Todos os computadores devem ter proteção de tela automática com senha habilitada para acionamento no tempo máximo de 5 minutos de inativação.

VIII – Senhas

O CRF-RJ adota política de troca obrigatória de senhas com período de uso contínuo de no máximo 30 (TRINTA) dias.

A senha é o meio de validação de acessos a recursos e serviços, funcionando como a assinatura digital do Colaborador, portanto, devem ser verificados os seguintes cuidados básicos para sua proteção:

(i) Manter sua confidencialidade;

(ii) Criar senhas fortes, respeitando, ao menos, os critérios abaixo:

a. As senhas não podem ser óbvias, como senhas sequenciais (ex.: sequências numéricas ou alfabéticas) ou derivadas de dados pessoais (ex.: nome ou data de nascimento do usuário), e;

b. Devem ter pelo menos 8 caracteres, com ao menos um caractere especial e um número.

Os acessos, validados por meio da utilização de senha, serão limitados aos recursos e serviços necessários para o desempenho das atividades exercidas por cada Colaborador, e poderão ser revogados rapidamente quando necessário.

IX - Cópias de Segurança (Backup)

A importância dos backups na administração de sistemas nunca pode ser minimizada. Sem eles, muitos dados são simplesmente irrecuperáveis caso sejam perdidos devido a uma falha acidental ou a um incidente de segurança.
Cada departamento/usuário tem acesso a pelo menos uma pasta no servidor e/ou serviço de nuvem de arquivos. Todos os documentos relacionados ao negócio devem ser armazenados nestas pastas. Além disso, cada usuário tem uma pasta individualizada para uso profissional noservidor e/ou serviço de nuvem de arquivos.

Qualquer arquivo armazenado em pastas locais nos computadores não é passível de backup, e por isso o armazenamento nesses locais é de total responsabilidade do usuário.

O backup dos servidores de aplicações e bancos de dados ocorre diariamente..

Termos e definições

OBJETIVO

Descrever termos e expressões usados na Política de Segurança da Informação, documentando de maneira clara quaisquer termos, classificações ou expressões, cujo significado possa causar dúvidas ou permitir interpretação diversa do que se pretende. Corresponde ao jargão utilizado pela Política de Segurança da Informação e precisa ser observado para que os normativos de segurança sejam entendidos.

PÚBLICO ALVO

Este normativo é destinado aos funcionários, conselheiros e terceirizados que exercem alguma atividade profissional no CRFRJ.

REFERÊNCIAS LEGAIS E NORMATIVAS

I - ABNT NBR 16167:2020 - Segurança da Informação — Diretrizes para classificação, rotulação e tratamento da informação.

II - ABNT NBR ISO 55000:2014 — Gestão de ativos — Visão geral, princípios e terminologia.

III - ABNT NBR ISO/IEC 27002:2013 — Tecnologia da Informação — Técnicas de Segurança — Código de Prática para controles de segurança da informação. IV -

Constituição da República Federativa do Brasil de 1988

V - Lei Federal nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências.

VI - Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

TERMOS E DEFINIÇÕES

1.1. Agentes de tratamento – o controlador e o operador (ref. Lei Federal 13.709/2018).

1.2. Anonimização – utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (ref. Lei Federal 13.709/2018).

1.3. Ativo – item, algo ou entidade que tem valor real ou potencial para uma organização (ref. ABNT NBR ISO 55000).

1.4. Ativos de informação - os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e os recursos humanos que a eles têm acesso.

1.5. Atributos biográficos – dados de pessoa natural relativos aos fatos da sua vida, tais como nome civil ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e vínculos empregatícios (ref. Decreto nº 10.046/2019).

1.6. Atributos biométricos - características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar (ref. Decreto 10046/2019)

1.7. Atributos genéticos – características hereditárias da pessoa natural, obtidas pela análise de ácidos nucleicos ou por outras análises científicas (ref. Decreto nº 10.046/2019).

1.8. Autoridade Classificadora – autoridade, designada pela organização, responsável pelas decisões no que diz respeito à classificação, à reclassificação, ao acesso e à proteção de uma informação sigilosa.

1.9. Classificação da informação – ação de definir o nível de sensibilidade da informação a fim de assegurar que a informação receba um nível adequado de proteção, conforme seu valor, requisitos legais, sensibilidade e criticidade para a organização (ref. NBR16167:2013)

1.10. Controlador – pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (ref. Lei Federal 13.709/2018).

1.11. Cracker – termo usado para designar quem pratica a quebra (ou cracking) de um sistema de TI, de forma ilegal ou sem ética.

1.12. Credencial (ou conta de acesso) – permissão, concedida por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso de recursos. A credencial pode ser física (como um crachá), ou lógica (como a identificação de usuário e senha).

1.13. Criticidade – nível de crise (ou impacto) que pode advir da divulgação ou uso indevido da informação (ref. NBR16167:2020).

1.14. Custodiante da informação ou custodiante – usuários, grupos de trabalho ou áreas delegadas pelo

proprietário do ativo de informação para cuidar da manutenção e guarda do ativo de informação no dia a dia.

1.15. Dado anonimizado – dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (ref. Lei 13.709/2018).

1.16. Dado pessoal – informação relacionada a pessoa natural identificada ou identificável (ref. Lei Federal 13.709/2018).

1.17. Dado pessoal sensível – dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (ref. Lei 13.709/2018).

1.18. Dados cadastrais – informações identificadoras perante os cadastros de órgãos públicos, tais como os atributos biográficos, o número de inscrição no Cadastro de Pessoas Físicas – CPF, o número de inscrição no Cadastro Nacional de Pessoas Jurídicas - CNPJ, o Número de Identificação Social – NIS, o número de inscrição no Programa de Integração Social – PIS, o número de inscrição no Programa de Formação do Patrimônio do Servidor Público – Pasep, o número do Título de Eleitor, a razão social, o nome fantasia e a data de constituição da pessoa jurídica, o tipo societário, a composição societária atual e histórica e a Classificação Nacional de Atividades Econômicas - CNAE e outros dados públicos relativos à pessoa jurídica ou à empresa individual (ref. Decreto nº 10.046/2019)

1.19. Encarregado – pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados – ANPD (ref. Lei Federal 13.709/2018)

1.20. Grupo de acesso – pessoas, grupos de trabalho ou áreas autorizadas a terem acesso à determinada informação (ref. NBR16167:2013).

1.21. Hoax – mensagem que tenta convencer o leitor de sua veracidade por um embuste ou farsa e depois tenta convencê-lo a realizar uma ação específica. A disseminação de um hoax depende do envio deliberado da mensagem à outras vítimas em potencial, que também fazem o mesmo

1.22. Informação – dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato (ref. Lei Federal nº 12.527/2011).

1.23. Informação de natureza pública – bem público, tangível ou intangível, com forma de expressão gráfica, sonora ou iconográfica, que consiste num patrimônio cultural de uso comum da sociedade e de propriedade das entidades/instituições públicas da administração centralizada, das autarquias e das fundações públicas. A informação de natureza pública pode ser produzida pela administração pública ou, simplesmente, estar em poder dela, para que esteja disponível ao interesse público ou coletivo da sociedade

1.24. Keylogger – Software que rastreia ou registra as teclas pressionadas em um teclado, geralmente de forma encoberta para que a pessoa usando o teclado não esteja ciente de que suas ações estão sendo monitoradas. Isso geralmente é feito por pessoas mal-intencionadas para coletar informações, incluindo mensagens instantâneas, textos e endereços de e-mail, senhas, números de cartões de crédito e contas bancárias, endereços e outros dados privado

1.25. Nível de classificação – categoria a ser definida para cada informação ou classe de informação, que estabelece a sensibilidade da informação em termos de preservação de sua confidencialidade, integridade e disponibilidade (ref. NBR16167:2013).

1.26. Operador – pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (ref. Lei Federal 13.709/2018).

1.27. Phishing – forma de fraude eletrônica, caracterizada por tentativas de adquirir dados pessoais, ao se fazer passar como uma pessoa confiável ou uma empresa enviando uma comunicação eletrônica oficial. Isto ocorre de várias maneiras, principalmente por e-mail, mensagem instantânea, SMS, dentre outros.

1.28. Privacidade – inviolabilidade do direito a intimidade, a vida privada, a honra e a imagem das pessoas (ref. Constituição da República Federativa do Brasil de 1988).

1.29. Proprietário do ativo de informação – refere-se à parte interessada do CRF-RJ, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação.

1.30. Proteção de dados pessoais – tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (ref. Lei Federal 13.709/2018).

1.31. Proxy anônimo – ferramenta que se esforça para fazer atividades na Internet sem vestígios: acessa a Internet a favor do usuário, protegendo as informações pessoais ao ocultar a informação de identificação do computador de origem.

1.32. Redes de bots ou botnet – Forma curta de "rede de robôs", é uma rede de computadores pirateados controlada remotamente por um hacker. O hacker pode usar a rede para enviar spam e lançar ataques de negação de serviço (DoS) e pode alugar a rede para outros cibercriminosos. Um único computador em um bonet pode automaticamente enviar milhares de mensagens de spam por dia. As mensagens de spam mais comuns vêm de computadores zumbis.

1.33. Relatório de impacto à proteção de dados pessoais (RIPD) – documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (ref. Lei Federal 13.709/2018).

1.34. Rótulo – identificação física ou eletrônica da classificação atribuída à informação.

1.35. Segurança da informação - implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware (ref. NBR 27002:2013).

1.36. Sensibilidade – grau de sigilo necessário para informação (ref. NBR16167:2013).

1.37. Smart card – cartão de plástico que geralmente assemelha-se em forma e tamanho a um cartão de

crédito convencional de plástico com um chip de computador embutido.

1.38. Spam – uma mensagem eletrônica indesejada, geralmente não solicitada, enviada por mala-direta. Normalmente, o spam é enviado para vários destinatários que não pediram para recebê-lo. Dentre os tipos de spam estão o spam por e-mail, spam por mensagens instantâneas, spam por mecanismos de pesquisa da Web, spam em blogs e spam por mensagens em telefones celulares. O spam pode conter publicidade legítima, publicidade enganosa e mensagens de phishing que tentam defraudar os destinatários para obter informações pessoais e financeiras. As mensagens não são consideradas spam caso o usuário tenha feito a solicitação para recebê- las.

1.39. Spyware – tipo específico de código malicioso. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Keylogger, screenlogger e adware são alguns tipos específicos de spyware.

1.40. Setor da Tecnologia e da Informação – ativo estratégico que suporta processos institucionais, por meio da conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, fazer uso e disseminar informações.

1.41. Termo de Classificação da Informação – Documento usado para formalizar a decisão da autoridade competente sobre a classificação da informação, que registra, entre outros dados, o nível de classificação, a categoria na qual se enquadra a informação, o tipo de documento, as datas da produção e da classificação, a indicação de dispositivo legal que fundamenta a classificação, as razões da classificação, o prazo de sigilo ou evento que definirá o seu término e a identificação da autoridade classificadora. O TCI deve ser anexado à informação classificada.

1.42. Titular – pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (ref. Lei Federal 13.709/2018).

1.43. Token – dispositivos físicos geradores aleatórios de código para uso como forma de autenticação.

1.44. Transparência ativa – princípio que exige de órgãos e entidades públicas a divulgação de informações de interesse geral, independentemente de terem sido solicitadas (ref. Lei 12527/2011).

1.45. Visão – declaração de propósito e futuro desejado, com perspectiva de longo prazo.

1.46. Backup: cópia exata de um programa, disco ou arquivo de dados feito para fins de arquivamentoou para salvaguardar informações