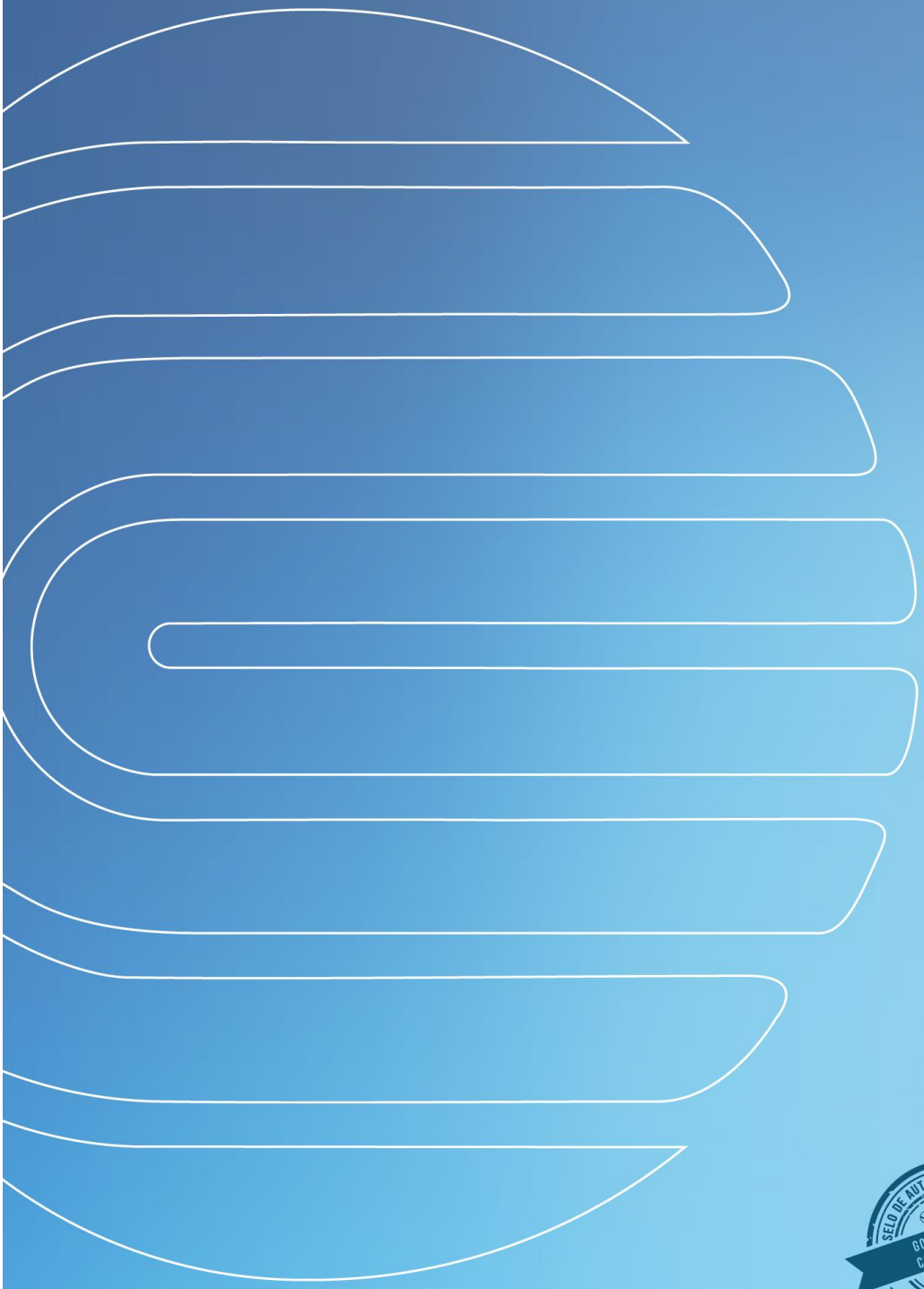
Regulamento de Segurança em Tecnologia da Informação e Comunicação - RSTIC



Sumário

Regulamento de Segurança em Tecnologia da Informação e Comunicação - RSTIC da Fundação Banco Central de Previdência Privada - Centrus

Capítulo I - Disposições Preliminares

Seção I - Objetivo

Art. 1º O presente regulamento tem por objeto o estabelecimento das normas gerais para utilização dos recursos do ambiente de Tecnologia da Informação e Comunicação - TIC da Centrus, a serem observadas por todos aqueles a quem seja autorizada a sua utilização.

Seção II - Definições

Art. 2º Definem-se, na aplicação deste regulamento:

I - administrador local: pessoa que tem total acesso ao computador, podendo efetuar alteração nas configurações, inclusive de segurança;

II - administrador de rede: empregado lotado na Gerência de Tecnologia da Informação - Geinf, responsável pela administração e manutenção de recursos da infraestrutura de TIC;

III - conta de identificação: código identificador do usuário nos recursos de TIC;

IV - conta de serviço: conta de identificação específica utilizada para a execução de serviços ou sistemas em recursos de TIC;

V - criptografia: método utilizado para codificação de arquivos de sua forma original para outra ilegível, de maneira a ser decodificado apenas por seu destinatário;

VI - dados ou informações sigilosos: dados ou informações cujo conhecimento irrestrito ou divulgação possa acarretar algum risco à segurança da Centrus, bem como aqueles necessários ao resguardo das estratégias operacionais, da inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas;

VII - Gesol - Sistema de Gestão de Solicitação de Serviço: sistema informatizado para registro e controle de autorização e de execução de serviço;

VIII - gestor: gerente responsável pela administração de sistema de TIC;

IX - instrumentos corporativos: equipamentos e mídias fornecidos ou homologados pela Centrus;

X - log: descrição do processo de registro de eventos relevantes em sistema computacional;

XI - mantenedor: colaborador lotado na Geinf responsável pelos serviços de instalação, configuração e manutenção dos recursos de TIC;

XII - sessão de trabalho: período em que o usuário, utilizando sua conta de identificação, fica conectado à rede de computadores;

XIII - usuário: pessoa que utiliza, de forma autorizada, os recursos do ambiente de TIC; e

XIV - mensagens suspeitas: são geralmente inesperadas, e buscam induzir seus destinatários a comportamentos impensados ou imediatos, levando-os por exemplo a clicar em links, abrir anexos ou preencher formulários maliciosos.

Art. 3º Conceitua-se, para efeito deste regulamento, no que se refere aos sistemas:

I - confidencialidade: capacidade de manter a informação disponível apenas para as pessoas devidamente autorizadas;

II - criticidade: grau de importância da informação para a continuidade dos negócios da Centrus;

III - disponibilidade: capacidade de manter serviços e recursos em plenas condições de uso, sempre que necessários;

IV - integridade: capacidade de manter desempenho correto, resguardando as informações, de forma que não possam ser destruídas ou corrompidas;

V - autenticidade: capacidade de assegurar que a informação em um sistema computacional seja verdadeira; e

VI - irretratabilidade: capacidade de garantir o não repúdio às informações fornecidas.

Seção III - Diretrizes

Art. 4º As normas de segurança em TIC devem ser conhecidas e seguidas pelos usuários da Centrus.

Art. 5º O ocupante de função gerencial deve zelar pelo cumprimento das diretrizes de segurança em TIC no âmbito de sua competência.

Art. 6º O usuário de recursos de TIC deve ter identificação pessoal e intransferível, exceto no acesso a recursos definidos pela Centrus como públicos.

Art. 7º Os recursos de TIC não podem ser utilizados para constranger, assediar, ofender, caluniar, ameaçar ou causar prejuízos a qualquer pessoa física ou jurídica, nem veicular opinião religiosa ou político-partidária.

Art. 8º O usuário terá acesso autorizado aos recursos de TIC, necessários e indispensáveis ao seu trabalho.

Art. 9º A Centrus deve assegurar que o usuário receba treinamento adequado à utilização dos recursos de TIC necessários à execução de sua tarefa.

Art. 10. A Centrus deve manter plano de contingência que garanta o fluxo de informações necessário à normalidade das atividades críticas.

Art. 11. A segurança deve ser direcionada contra destruição, modificação ou divulgação indevida de informações, quer acidental, quer intencional.

Art. 12. O usuário, ao acessar os recursos de TIC, deve considerar que eles possuem disponibilidade limitada.

Seção IV - Dados e Informações

Art. 13. A utilização de recursos de TIC e o acesso a informações da Centrus neles disponibilizados, exceto as de domínio público, estão condicionados ao aceite deste regulamento, por meio:

I - de cláusula constante no contrato de trabalho, para os empregados;

II - por meio do respectivo termo de posse, para os diretores e conselheiros; e

III - de formulário impresso, para estagiários, cedidos e prestadores de serviço, que será arquivado na Gerência de Contabilidade e Logística - Gecon ou, no caso dos prestadores de serviços, na Geinf.

Parágrafo único. O acesso aos recursos de TIC sem o aceite de que trata o *caput* pode configurar invasão ao ambiente corporativo, com a consequente apuração de conduta ao infrator sob o aspecto ético e funcional, sem prejuízo de outras sanções cabíveis daí decorrentes.

Art. 14. As informações sigilosas, disponibilizadas em meio eletrônico para acesso ou manuseio fora das dependências da Centrus, independentemente do meio ou da mídia, devem estar protegidas por senhas, sistemas de leitura facial, digital ou por mecanismo de criptografia, de forma a garantir os aspectos básicos da segurança da informação.

§ 1º A Centrus deve disponibilizar ferramenta de criptografia para os microcomputadores portáteis e os dispositivos de armazenamento.

§ 2º As informações consideradas sigilosas deverão trafegar apenas por meio de instrumentos corporativos.

§ 3º As informações de caráter corporativo não podem ser armazenadas em dispositivos sem backup corporativo.

Capítulo II - Responsabilidades, Atribuições e Competências

Seção I - Responsabilidades

Art. 15. É de responsabilidade do usuário:

I - a utilização idônea de sua conta de identificação na rede de computadores;

II - a manutenção do sigilo e a não utilização privada de informações geradas, adquiridas ou utilizadas pela Centrus, às quais tenha tido acesso no exercício de suas atividades;

III - a manutenção do sigilo das suas senhas de acesso aos recursos, aos sistemas e aos serviços da rede de computadores;

IV - a segurança das informações armazenadas nos recursos de TIC, especialmente quando do download de arquivos, com vistas a evitar ataques de vírus e demais ameaças invasivas;

V - o acesso realizado com sua conta de identificação na rede de computadores;

VI - o armazenamento de arquivos pessoais em locais apropriados, vedada a hospedagem em equipamentos servidores de rede local;

VII - as opiniões pessoais emitidas em ambientes virtuais por meio de e-mail, de redes sociais ou de qualquer outro veículo;

VIII - o encerramento da sessão de trabalho ou o seu bloqueio com senha de acesso, ao afastar-se da estação de trabalho;

IX - o cuidado e o zelo no manuseio da sua estação de trabalho e dos demais recursos de TIC a que tiver acesso; e

X - trocar sua senha de acesso à rede de computadores imediatamente após recebê-la.

Art. 16. É vedado ao usuário utilizar os recursos de TIC para:

I - promover atividade comercial própria ou de terceiros, incluindo oferta de serviços ou de produtos, salvo por meio de canais institucionais adequados;

II - enviar mensagens:

a) cuja fonte primária não tenha sido confirmada;

b) contendo vírus ou qualquer forma de rotina de programação prejudicial ou danosa às estações de trabalho ou ao sistema de e-mail;

c) que contribua para a continuidade de correntes de mensagens eletrônicas;

d) com informação sigilosa ou corporativa para pessoa não autorizada;

e) com conteúdo ofensivo; e

f) que, de alguma forma, viole a legislação em vigor;

III - ler ou tentar ler mensagem de outro usuário sem expressa autorização; e

IV - executar jogos, exceto aqueles disponibilizados pelos canais e pelas ferramentas institucionais.

Art. 17. O usuário deve informar à Geinf, imediatamente, qualquer suspeita de:

I - eventual dano causado às informações armazenadas nos equipamentos servidores da rede de computadores;

II - quebra de sigilo da senha de acesso individual, providenciando imediatamente a sua troca;

III - contaminação de arquivos ou dispositivos por vírus de computador; e

IV - falha de segurança ou vulnerabilidade detectada no ambiente de TIC.

Art. 18. O usuário com permissão adicional de mantenedor ou de administrador de rede somente pode acessar os dados e as informações estritamente necessários à execução dos seus trabalhos.

Seção II - Atribuições

Art. 19. É atribuição dos empregados lotados na Geinf atuar como administrador local.

Parágrafo único. O Diretor de Controle, Logística e Informação - Diaco pode autorizar a empregado não lotado na Geinf a atribuição de que trata o *caput*, quando necessária à execução de suas atividades.

Art. 20. São atribuições do gerente:

I - garantir o cumprimento das diretrizes de segurança em TIC no âmbito da respectiva gerência;

II - autorizar, por meio de Gesol, o acesso às informações e aos recursos de que é gestor, definindo, quando for o caso, as datas de início e de fim de sua utilização;

III - solicitar ajustes e aprimoramentos nos sistemas de TIC sob sua gestão;

IV - manter atualizada a relação de usuários a ele subordinados; e

V - autorizar a entrada e a saída de recursos de TIC na respectiva gerência.

Art. 21. É atribuição específica do gerente da Gecon comunicar à Geinf, por meio de Gesol, o desligamento de empregado, de conselheiro, de cedido, de estagiário ou de contratado.

Seção III - Competências

Art. 22. Cabe à Geinf:

I - prestar apoio técnico à Diretoria-Executiva - Direx na formulação e na atualização da política de segurança de TIC;

II - desenvolver estudos e emitir pareceres para orientar aquisições de hardware e de software no âmbito da Centrus;

III - prestar apoio técnico na definição das prioridades no desenvolvimento de soluções internas com recursos de TIC;

IV - promover ações destinadas à disseminação das melhores práticas de utilização dos recursos de TIC;

V - elaborar e validar planos de continuidade de negócios que envolvam recursos de TIC;

VI - propor o estabelecimento de sanções pelo não cumprimento de normas relativas à segurança em TIC;

VII - administrar, gerenciar e manter a infraestrutura e as respectivas soluções de disponibilidade das áreas de armazenamento, compreendendo equipamentos servidores e dispositivos de armazenamento;

VIII - manter íntegros informações e dados corporativos criados e guardados pelos usuários nas áreas de armazenamento adequadas para esse fim;

IX - testar periodicamente as cópias dos dados armazenados para fins de segurança;

X - assegurar a disponibilidade e a integridade dos recursos de TIC;

XI - prover aos usuários o apoio necessário à implementação e à compreensão das diretrizes de segurança em TIC;

XII - prover aos usuários apoio técnico à adequada utilização dos recursos de TIC;

XIII - realizar ações de divulgação e de conscientização dos usuários para a correta utilização dos recursos de TIC;

XIV - manter sistemas e ferramentas de segurança corretamente instaladas e operacionais;

XV - monitorar e mitigar vulnerabilidades na rede de computadores;

XVI - realizar verificações periódicas objetivando avaliar o cumprimento deste regulamento;

XVII - testar e homologar todos os softwares e os equipamentos antes de sua instalação;

XVIII - gerenciar o sistema de cópia de segurança das informações armazenadas em recursos de TIC;

XIX - preservar em local seguro contra danos e extravio as cópias de segurança das informações armazenadas em recursos de TIC da Centrus;

XX - credenciar as contas de identificação dos usuários e o acesso aos recursos de TIC, conforme autorização das áreas pertinentes;

XXI - gerenciar as contas de identificação dos usuários nos sistemas de rede e nos aplicativos;

XXII - alterar permissões de acesso a arquivos e a aplicativos solicitadas pelas gerências por meio de Gesol; e

XXIII - liberar, bloquear, desbloquear ou cancelar conta de identificação de usuário.

Capítulo III - Procedimentos Operacionais

Seção I - Contas e Senhas

Art. 23. Todo acesso a área restrita e a recursos internos de TIC da Centrus deve ser identificado e autenticado.

Art. 24. As contas de identificação são divididas em contas de uso individual, contas administrativas e contas de serviço.

Art. 25. O usuário deve verificar, ao digitar sua conta e senha de rede em um sistema, se este corresponde a um sistema da Centrus.

Art. 26. As senhas:

I - não devem ficar desprotegidas ou em local visível; e

II - não devem ser enviadas por meio inseguro, como e-mail, Teams e outros.

Art. 27. As senhas da conta de uso individual e da conta administrativa de rede não devem ser compartilhadas em nenhuma hipótese.

Art. 28. Não se deve reutilizar as senhas da rede da Centrus em contas de sites e serviços na Internet.

Seção II - Contas de uso individual

Art. 29. Todo funcionário, membro de órgão estatutário, preposto de órgão fiscalizador, prestador de serviço e estagiário em atividade na Centrus que necessitar de acesso a algum recurso de TIC da Centrus terá uma conta de uso individual, ressalvados casos especiais em função da necessidade do serviço.

Art. 30. A conta de uso individual é de uso pessoal, exclusiva e intransferível.

Art. 31. O usuário é responsável por todos os acessos realizados com sua conta de uso individual.

Art. 32. A senha da conta de uso individual:

I - precisa ter caracteres alfanuméricos, sendo o formato e o tempo de validade definidos pela Geinf;

II - a conta é bloqueada caso a senha seja informada incorretamente por cinco vezes seguidas; e

III - usuários visitantes que necessitem de acesso à Internet devem ter conta de uso individual cadastrada.

Art. 33. O usuário perderá o acesso aos recursos de TIC:

I - no caso de desligamento da Centrus, se empregado; e

II - ao final da relação de vínculo empregatício ou de atividade na Fundação, nos demais casos.

Art. 34. As contas de uso individual de usuários temporários deverão ter prazo de utilização determinado, podendo ser prorrogado em função da necessidade do serviço.

Art. 35. A utilização da conta de uso individual por terceiro, com ou sem conhecimento do usuário, configura uso indevido ou abusivo de dados e de informações e sujeita os envolvidos às sanções previstas na legislação em vigor.

Art. 36. As solicitações de liberação, de bloqueio, de desbloqueio ou de cancelamento de acesso aos recursos de TIC devem ser formalizadas por meio de Gesol, ressalvados os casos de bloqueio acidental de contas.

Seção III - Contas administrativas

Art. 37. Atividades que exijam privilégio administrativo em recursos de TIC devem utilizar conta administrativa.

Art. 38. As contas administrativas não têm acesso à Internet ou a e-mail de alcance externo.

Art. 39. A administração de recursos de TIC, com exceção das estações de trabalho, será feita exclusivamente por técnicos da Geinf.

Art. 40. A senha da conta administrativa de rede:

I - não é sincronizada com a da conta de uso individual;

II - precisa ter no mínimo 12 caracteres, sem limite superior, e deve ser formada por, no mínimo, 3 dos seguintes requisitos: letras minúsculas, letras maiúsculas, números e caracteres especiais; e

III - deve ser trocada pelo usuário, pelo menos, a cada 365 dias.

Art. 41. A conta administrativa de rede será excluída quando o funcionário ou prestador de serviço mudar de localização.

Seção IV - Contas administrativas locais

Art. 42. A respeito de contas administrativas locais de estação de trabalho:

I - não é permitido o logon remoto com contas administrativas locais; e

II - é vedada a criação de contas administrativas locais adicionais.

Art. 43. As senhas de contas administrativas locais de servidores deverão ser trocadas anualmente; e sempre que houver desligamento de algum integrante da equipe da Geinf com conhecimento das senhas.

Art. 44. As contas administrativas locais só devem ser utilizadas quando não for possível o uso da conta administrativa de rede.

Seção V - Contas de serviço

Art. 45. As contas de serviço são utilizadas em programas, aplicações ou sistemas que necessitem acesso a recursos de TIC da Centrus.

Art. 46. A conta de usuário de serviço é criada pela Geinf, sua senha não expira, é gerada de forma aleatória e disponibilizada de maneira segura e exclusiva aos responsáveis/solicitantes.

Art. 47. As contas de serviço não devem ser utilizadas para efetuar logon interativo em estação de trabalho.

Seção VI - Contas de perfis institucionais na Internet

Art. 48. São exemplos de perfis institucionais as contas da Centrus no Facebook, no Linkedin, no Instagram e no Whatsapp, entre outros.

Art. 49. Cada perfil institucional da Centrus na Internet deve ter como gestor um funcionário nomeado como Agente Responsável.

Art. 50. É vedada a terceirização completa da administração e da gestão de perfis da Centrus na Internet.

Art. 51. Deve ser configurada autenticação por dois fatores para acesso ao perfil sempre que essa funcionalidade estiver disponível. Autenticação por dois fatores é aquela em que um segundo elemento, além da senha, é verificado no momento do acesso à conta. São exemplos o envio de SMS para telefone celular, disponível no X, e o uso do Google Authenticator, disponível no Youtube.

Seção VII - Utilização de Hardware

Art. 52. As estações de trabalho são protegidas contra violações físicas, por meio de lacre colocado pelo mantenedor.

§ 1º Não devem ser lacrados os equipamentos instalados na Centrus de propriedade de empresas prestadoras de serviços.

§ 2º O lacre de segurança somente pode ser removido pelo mantenedor.

§ 3º O usuário deve certificar-se de que o equipamento sob sua guarda contém o lacre de segurança, ao recebê-lo e no retorno de serviço de manutenção.

§ 4º A inexistência ou a apresentação de sinal de violação do lacre de segurança deve ser prontamente reportada à gerência correspondente e à Geinf.

Art. 53. Não é permitida a conexão simultânea de estação de trabalho ou de outros equipamentos à rede de computadores e a modens USB.

Art. 54. Recursos de TIC de terceiros somente podem ser conectados à rede de computadores após adequação aos padrões internos da Centrus e respectiva homologação pela Geinf.

Art. 55. A manutenção de equipamentos de hardware deve ser realizada pelo mantenedor e acompanhada por usuário da gerência solicitante.

§ 1º A remoção de equipamento do local de atendimento, para manutenção ou substituição, somente pode ser efetuada após autorização do usuário responsável pela sua utilização ou de sua chefia imediata.

§ 2º Caso necessário o envio de equipamentos, toda mídia que contenha informação sigilosa deve ser removida pelo mantenedor, após autorização do usuário ou de sua chefia imediata, e mantida sob a guarda da Geinf até o retorno do equipamento.

Art. 56. Em caso de venda ou de doação de computador, o disco rígido deve ser formatado com o objetivo de inutilizar as informações nele gravadas.

Art. 57. A localização dos equipamentos computacionais na Centrus deve ser objeto de controle específico.

Seção VIII - Utilização de Software

Art. 58. A instalação ou a configuração de software nas estações de trabalho somente deve ser realizada pela Geinf, componente responsável pela guarda das mídias e pela desinstalação, quando necessária.

Seção IX - Uso de Equipamentos Móveis

Art. 59. As configurações dos equipamentos móveis para conexão à rede de computadores e os meios de conexão devem obedecer às especificações estabelecidas pela Geinf.

Art. 60. Os equipamentos móveis corporativos devem contar com proteção contra acesso não autorizado e ser utilizados com precaução contra roubo e furto.

Seção X - Acesso remoto a recursos de TIC internos da Centrus a partir de rede externa

Art. 61. Recursos de TIC internos da Centrus podem ser acessados remotamente a partir de rede externa por meio de conexão segura com autenticação por dois fatores.

Art. 62. Recursos específicos podem ter acesso permitido sem autenticação por dois fatores se a implementação for operacionalmente inviável.

Art. 63. A conexão segura deve ser feita a partir de equipamentos corporativos.

Art. 64. Todas as operações realizadas durante o acesso remoto poderão ser monitoradas por meio de arquivo de log.

Art. 65. O acesso remoto temporário, a partir de rede externa, para fins de suporte a serviço, tecnologia, ferramenta ou produto localizado na rede interna da Centrus é permitido apenas com o acompanhamento de toda a sessão pelo usuário que demandou o suporte, que deve garantir, após seu término, que a sessão seja devidamente encerrada e desconectada.

Seção XI - Conexão de equipamentos corporativos a redes de terceiros

Art. 66. Por conexão de equipamentos corporativos a redes de terceiros entende-se a conexão local via cabo ou rede Wi-Fi.

Art. 67. Se for necessária a conexão de equipamentos corporativos a redes de terceiros, ela deve observar as seguintes diretrizes:

I - não se deve instalar, em nenhuma hipótese, softwares, aplicativos ou drivers para conexão à rede. Se este for um requisito para conexão à rede, o equipamento não deverá ser conectado; e

II - ao acessar algum recurso de TIC da Centrus utilizando-se redes de terceiros, deve-se observar se o certificado digital para acesso à aplicação é confiável. Se houver algum alerta indicando que o certificado não é confiável, o usuário não deve prosseguir.

Seção XII - Correções de segurança

Art. 68. São aplicadas correções de segurança:

I - mensalmente, no caso de servidores com sistema operacional Windows;

II - bimestralmente, no caso de servidores com sistema operacional Linux; e

III - sempre que houver correção crítica para servidores e ativos com outro sistema operacional.

Art. 69. O ciclo de aplicação das correções pode ser antecipado em caso de correção de segurança considerada emergencial.

Art. 70. Nas estações de trabalho, são aplicadas correções de segurança assim que publicadas, ao menos nos seguintes softwares: Microsoft Windows, Microsoft Office, Adobe Reader, Adobe Flash Player e navegadores.

Art. 71. O Java Runtime Environment é atualizado após homologação da nova versão pela Geinf.

Seção XIII - Soluções de computação em nuvem

Art. 72. Apenas as soluções de computação em nuvem contratadas pela Centrus podem ser utilizadas para apoio de processos corporativos relevantes, bem como para o armazenamento de informações de acesso restrito.

Art. 73. São exemplos de soluções de computação em nuvem:

I - webmail;

II - blogs (ex: BlogSpot);

III - sites de compartilhamento de mídia (ex: Youtube);

IV - sites para armazenamento, compartilhamento e sincronização de arquivos (ex: iCloud, DropBox, 4shared, Google Drive, Onedrive);

V - sites para compartilhamento e controle de versão de código-fonte (ex: Google Code, GitHub);

VI - sites para conversão, edição ou assinatura de documentos (Docusign, iLovePDF, JPGtoPDF); e

VII - outras ferramentas (ex: Evernote, Yummie, Trello, Prezi).

Capítulo IV – Uso de informações e internet

Seção I - Armazenamento em estações de trabalho ou dispositivos móveis

Art. 74. O usuário é responsável pelas informações armazenadas na estação de trabalho e nos demais dispositivos móveis que utilizar para o desempenho de suas atribuições.

§ 1º A Geinf não é responsável pela cópia de segurança, nem pela integridade de dados e de informações armazenados em estações de trabalho ou em dispositivos móveis.

§ 2º As informações armazenadas nas estações de trabalho podem ser acessadas pela Consultoria Jurídica - Cojur, ou pelo Comitê de Ética da Centrus - CEC, no âmbito de procedimento disciplinar devidamente instaurado, independentemente de alegação de privacidade das informações.

Seção II - Armazenamento de arquivos eletrônicos corporativos

Art. 75. Os arquivos eletrônicos corporativos não podem ser armazenados em estações de trabalho ou equipamentos portáteis.

Art. 76. Os arquivos eletrônicos corporativos podem ser armazenados no Servidor de arquivos, no OneDrive ou no Teams

Art. 77. Os servidores de arquivos da Fundação terão áreas de armazenamento reservadas para cada gerência.

Art. 78. É responsabilidade da Geinf a realização periódica de cópias de segurança dos arquivos corporativos armazenados nos servidores de arquivos.

Art. 79. É responsabilidade da Unidade assegurar o uso correto e eficiente da área de armazenamento reservada a ela, verificando periodicamente se não existem arquivos que infrinjam direitos autorais ou que apresentem outros riscos jurídicos, como músicas, filmes e livros que não tenham sido adquiridos pela Centrus.

Seção III - Cópia de segurança

Art. 80. O tempo de retenção da cópia de segurança das informações armazenadas nos equipamentos gerenciados pela Geinf será definido de acordo com os prazos regulamentares.

Art. 81. A restauração da cópia de segurança de informações, quando necessária, deve ser solicitada por meio de Gesol à Geinf.

Art. 82. Para o armazenamento ou o descarte de informações corporativas, o usuário deve seguir as orientações da Geinf, observado que:

I - o armazenamento de informação considerada sigilosa deve ser realizado em pasta de equipamento servidor de rede com acesso restrito; e

II - o método de descarte de informação sigilosa deve impedir sua recuperação total ou parcial.

Seção IV - Proteção Lógica das Informações

Art. 83. As estações de trabalho e os equipamentos servidores de rede devem estar protegidos contra ataques de vírus e de software mal-intencionado, na forma definida pela Geinf.

Art. 84. É vedada a abertura de arquivos suspeitos ou originados de remetente desconhecido.

Art. 85. O processo de atualização de software antivírus deve ser realizado automaticamente nas estações de trabalho e nos equipamentos servidores de rede.

Art. 86. O software antivírus deve efetuar automaticamente a procura por vírus em todos os dados armazenados ou trafegados nos recursos de TIC.

Art. 87. O software antivírus deve bloquear automaticamente todos os dados armazenados ou trafegados nos recursos de TIC com suspeita ou confirmação de presença de vírus.

Seção V - Acesso à Internet

Art. 88. Todo acesso à internet deve ser identificado e registrado.

Art. 89. Em caso de suspeita de incidente de segurança, a Geinf deve bloquear o acesso à internet para usuários e para estações de trabalho da rede.

Art. 90. O acesso a sítios e a serviços, principalmente de conteúdo multimídia, na internet (youtube, rádio, TV etc), deve ser efetuado em função:

I - da capacidade operacional da rede de computadores e de aspectos de segurança; e

II - da necessidade funcional da área demandante.

Parágrafo único. A Geinf deve:

I - utilizar software específico de filtro de conteúdo para bloqueio a sítios e a serviços de internet considerados inadequados para acesso; e

II - bloquear o acesso a sítios que atentem contra a segurança da rede de computadores ou contra as normas internas e externas aplicáveis à TIC.

Capítulo V - Uso de e-mail

Seção I - Contas de e-mail

Art. 91. As contas de e-mail corporativo podem ser de uso individual ou departamental, por caracterizar estrutura formal ou projeto da Centrus.

Art. 92. Todo empregado ou membro de órgão estatutário tem conta de e-mail individual de alcance externo, criada após a assinatura do Termo de Sigilo e de Responsabilidade do RSTIC. Ao desligar-se, o empregado ou o membro de órgão estatutário perderá acesso ao e-mail corporativo.

Art. 93. Os prestadores de serviço podem ter conta de e-mail de alcance interno ou externo, criada mediante solicitação formal à Geinf.

Art. 94. As mensagens de interesse do serviço devem incluir a assinatura eletrônica do usuário, conforme modelo disponibilizado pela Gerência de Comunicação e Relacionamento - Gecor.

Art. 95. O usuário de e-mail não deve usar o serviço para o envio de dados sensíveis, como senha, número de conta, informação sigilosa, salvo se estiver em consonância com as regras definidas pela Geinf.

Art. 96. Cabe à Geinf definir, observadas as características técnicas e operacionais da Centrus, os limites máximos de:

I - tamanho de mensagem de e-mail, incluindo seus anexos;

II - tamanho da caixa postal corporativa departamental e individual; e

III - quantidade de destinatários por mensagem.

Seção II - Conteúdo das mensagens

Art. 97. O conteúdo das comunicações via e-mail é considerado propriedade da Centrus, não havendo privacidade em relação a este material.

Art. 98. Não é recomendado o uso de pastas particulares, pois elas acarretam potenciais problemas de disponibilidade e segurança das mensagens.

Seção III - Uso do e-mail

Art. 99. As contas de e-mail somente deverão ser utilizadas para troca de mensagens relacionadas com o serviço.

Art. 100. O e-mail corporativo não deve ser usado para cadastro em sites de terceiros, exceto quando imprescindível.

Art. 101. É vedado ao usuário utilizar os sistemas de e-mail da Centrus para enviar mensagens não-institucionais para grupos ou pessoas que não as solicitaram ou autorizaram (spam).

Art. 102. A Centrus se reserva o direito de bloquear mensagens ou de colocá-las em quarentena, para a verificação de riscos, de acordo com os critérios definidos pela Geinf.

Art. 103. A Centrus se reserva o direito de desativar qualquer conta de e-mail ou alterar qualquer endereço de e-mail como salvaguarda a ataques por e-mail.

Art. 104. O serviço de e-mail só pode ser utilizado para troca de informações sensíveis se for utilizada criptografia da mensagem ou dos anexos.

Art. 105. É vedado ao usuário encaminhar ou redirecionar e-mails corporativos da Centrus, para endereços de e-mail pessoais.

Seção IV - Programas computacionais

Art. 106. Os programas computacionais devem ser previamente autorizados para envio de e-mail.

Art. 107. O programa computacional é responsável por tratar eventuais erros de envio das mensagens.

Seção V - Listas de distribuição com destinatários externos

Art. 108. O gerenciamento das listas de distribuição com destinatários externos (inclusão de destinatários) é responsabilidade da Unidade gestora.

Art. 109. Recomenda-se que as listas de distribuição com destinatários externos sejam moderadas.

Art. 110. As pessoas devem preferencialmente optar por entrar na lista e as mensagens da lista devem conter informações de como sair dela.

Seção VI - Acesso remoto à conta de e-mail por equipamento particular

Art. 111. Ao acessar remotamente a conta de e-mail por equipamento particular, é responsabilidade do usuário garantir a segurança do equipamento e das informações acessadas.

Art. 112. São controles de segurança recomendados:

I - o antivírus;

II - o bloqueio de tela;

III - a atualização frequente do sistema operacional e dos aplicativos;

IV - a criptografia/codificação;

V - a utilização apenas de fontes de aplicativos seguras; e

VI - que o dispositivo não tenha passado por procedimento de jailbreaking, rooting ou similar.

Art. 113. Ao configurar o dispositivo móvel particular para acesso ao e-mail da Centrus, o usuário autoriza a Centrus a apagar todos os dados do dispositivo remotamente em caso de perda, furto, roubo ou por solicitação do usuário, quando tecnicamente viável.

Seção VII - Mensagens suspeitas

Art. 114. O usuário não deve clicar em links ou abrir anexos de mensagens suspeitas.

Art. 115. Mensagens suspeitas devem ser encaminhadas à Geinf através do endereço email.suspeito@centrus.org.br.

Capítulo VI - Uso de certificado digital

Art. 116. A assinatura eletrônica é o padrão utilizado pela Centrus, sendo a exceção a assinatura em papel.

Art. 117. O uso de assinatura eletrônica com a utilização ou não de certificado digital deve observar às orientações emanadas da Cojur.

Art. 118. Os certificados digitais devem ser válidos pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Art. 119. Os certificados digitais utilizados para Identificação e Autenticação devem ser do tipo A1 ou A3.

Art. 120. O certificado e-CNPJ ficará sob a custódia do Diretor-Presidente da Centrus.

Art. 121. O monitoramento do prazo de expiração é responsabilidade do proprietário do certificado.

Art. 122. O monitoramento do prazo de expiração e-CNPJ fica a cargo da Gecon.

Seção I - Monitoramento e da Auditoria de Segurança

Art. 123. O uso dos recursos de TIC deve ser monitorado com geração de arquivo de log.

Capítulo VII - Disposições finais

Art. 124. Qualquer infração ou suspeita de infração a este regulamento deve ser comunicada imediatamente à Geinf.

Parágrafo único. O descumprimento ao disposto neste regulamento pode implicar ao infrator restrição ou perda, temporária ou permanente, do direito de acesso à rede de computadores e a outros recursos de TIC, independentemente da aplicação de penalidades previstas em lei e nas normas disciplinares da Centrus.

Art. 125. A Geinf pode suspender, preventiva e temporariamente, o acesso a recursos de TIC sempre que julgar necessário à preservação da integridade das informações ou dos equipamentos.

Parágrafo único. A suspensão de que trata o caput pode ser adotada, em caráter preventivo, na ocorrência de suspeita de infração a este regulamento.

Art. 126. Os casos omissos devem ser submetidos à apreciação do Diaco.

Art. 127. Este Regulamento entra em vigor em 1º de julho de 2024, devendo ser amplamente divulgado a todos os usuários.

Anexo ao Regulamento de Segurança em Tecnologia da Informação e Comunicação – RSTIC

Termo de Sigilo e de Responsabilidade

Para os fins previstos no art. 13 do Regulamento de Segurança em Tecnologia da Informação e Comunicação - RSTIC da Fundação Banco Central de Previdência Privada - Centrus, firmo este termo, declarando-me plenamente ciente das disposições do referido regulamento, em especial que:

I - o acesso à rede de computadores da Centrus, por qualquer equipamento ou dispositivo e independentemente do meio de comunicação, é regido pelas disposições do RSTIC, em face do que assumo, neste ato, toda a responsabilidade e as obrigações ali previstas; e

II - o uso indevido ou fraudulento dos recursos de TIC enseja apuração de responsabilidade, na forma das normas em vigor.

Aprovação:

Ata 2024/14, de 19 de junho de 2024: atualização.

Centrus

0800 704 0494
www.centrus.org.br
relacionamento@centrus.org.br
(61) 9 8138 8995