POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

NR Nº 001/2020 – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

Os recursos de informação do Cibrius, incluindo dados, documentos, aplicações, sistemas, hardware, ativos de redes e software, são ativos valiosos para o Instituto. Esses ativos estão sujeitos a riscos decorrentes de ameaças como erro de colaboradores, falhas de hardware, desastres naturais e ações criminosas ou mal-intencionadas. Tais eventos podem resultar em prejuízos causados pela perda de integridade e precisão dos dados, destruição ou divulgação indevida de informações e pela interrupção dos serviços de processamento de dados.

A Política de Segurança da Informação é um documento que fornece a base para a implementação bem-sucedida de medidas de proteção da informação, tendo em vista a redução dos riscos a níveis aceitáveis para a organização. O desenvolvimento e implementação de uma política de segurança é extremamente benéfica, não só por possibilitar a inclusão de todos os membros da organização nos esforços de proteger as informações e comunicações corporativas, mas também por reduzir a probabilidade de ocorrência de erros provocados pelo "fator humano" nos processos organizacionais, cujas consequências podem ser a divulgação de informações para pessoas não autorizadas, o uso inseguro ou inadequado da Internet e a realização de outras ações indevidas que tragam prejuízos para a organização.

Adicionalmente, o processo de definição da Política de Segurança da Informação ajuda o Cibrius a identificar seus ativos informacionais críticos e as formas pelas quais eles precisam ser protegidos, possibilitando a concentração dos esforços nas medidas de proteção mais eficientes e eficazes.

2. DO OBJETIVO

2.1. Possibilitar o gerenciamento da segurança da informação no Cibrius, estabelecendo regras e padrões para sua proteção, a partir do entendimento e documentação dos processos, da identificação dos requisitos de segurança baseados na análise de riscos e do desenvolvendo normas e processos de segurança da informação.

3. DA APLICAÇÃO

3.1. Esta Política aplica-se às atividades de todos os usuários dos sistemas e recursos de informação do Cibrius, incluindo membros dos órgãos estatutários, empregados do quadro próprio ou cedidos e prestadores de serviços.

4. DAS CONCEITUAÇÕES

4.1. **Backup:** cópia de segurança de arquivos de dados, informações e configurações de hardware e software mantida para permitir a recuperação dos dados originais em caso de falha ou indisponibilidade do sistema.

4.2. **Dado:** registro ou fato em sua forma primária, usado para representar uma quantidade, um objeto etc.

4.3. **Firewall:** barreira colocada entre um computador ou rede interna e o ambiente externo para proteção do ambiente interno contra acesso indevido aos recursos de informação.

4.4. **Gestor da informação:** gestor responsável pela área em que é produzida e/ou tratada a informação (ex.: gerente de benefícios = gestor da informação sobre benefícios; gerente de investimentos = gestor da informação sobre investimentos).

4.5. **Informação:** resultado da organização ou combinação de dados de forma significativa e contextual. Pode estar registrada em papel ou armazenada eletronicamente, ser mostrada em filmes ou falada em uma conversa.

4.6. **Infraestrutura de TI:** conjunto de dispositivos de hardware, equipamentos, redes, mídias de armazenamentos, bases de dados e software que dá suporte aos sistemas e aplicações baseadas em TI.

4.7. **Log:** registro histórico que armazena informações sobre as ações realizadas pelo usuário, tais como identidade do usuário, operações realizadas, data e hora, recursos acessados.

4.8. **Patch:** correção temporária de problemas detectados em código de software, liberada antes da conclusão de uma correção definitiva a ser ofertada na próxima versão do programa.

4.9. **Consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada

4.10. **Tratamento de dados:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

4.11. **Dado Pessoal:** informação relacionada a pessoa natural identificada ou identificável ou qualquer informação que identifique ou possa identificar uma pessoa física, tais como nomes, números, códigos de identificação, endereços, imagens (fotos).

4.12. **Dados pessoais sensíveis:** informações sobre origem racial ou étnica, convicção religiosa, opinião pública, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou vida sexual, dado genético ou biométrico quando vinculado à uma pessoa natural.

4.13. **Segurança da informação:** processo de preservar a informação levando em conta os seguintes objetivos:

4.13.1. **Confidencialidade:** garantia de que o acesso à informação é restrito aos seus usuários legítimos.

4.13.2. **Integridade:** garantia da criação da informação livre de erro e da proteção contra sua adulteração.

4.13.3. **Disponibilidade:** garantia de que a informação esteja disponível para os usuários legítimos de forma oportuna.

4.14. Sistema: conjunto de elementos ou componentes que interagem para produzir resultados previamente definidos. Os sistemas são compostos de entradas, saídas e mecanismos de processamento e feedback ou retroalimentação.

4.15. Sistema de informação: sistema que processa informações (pode ser manual ou informatizado).

4.16. Sistema de informação baseado em tecnologia da informação: sistema de informação que se vale de recursos de informática para efetuar um ou mais processos relacionados ao ciclo de vida da informação (coleta ou geração, tratamento, armazenamento, distribuição etc.).

4.17. Tecnologia da informação (TI): solução ou conjunto de soluções sistematizadas baseadas no uso de métodos, recursos de informática, de comunicação e de multimídia que visam a resolver problemas relativos à geração, tratamento, processamento, armazenamento, veiculação e reprodução de dados e a subsidiar processos que convertem dados em informação.

4.18. Usuário: colaborador, membro de conselho, prestador de serviços, estagiário, representante de fornecedor ou qualquer outro indivíduo que concorra para a realização do trabalho na Cibrius, ao qual tenha sido concedido acesso aos recursos de informação e tecnologia da organização.

5. DOS CRITÉRIOS E PROCEDIMENTOS

5.1. Controle de Acesso

5.1.1. Cabe ao usuário:

5.1.1.1. Manter o sigilo das informações confidenciais às quais tenha acesso e de suas senhas de acesso aos recursos computacionais do Cibrius;

5.1.1.2. Efetuar a troca das senhas de acesso sempre que solicitado pelo sistema ou pela ÁREA DE INFORMÁTICA, ou quando houver a suspeita de que estas não estejam mais seguras; e

5.1.1.3. Bloquear o acesso de terceiros às informações sob sua responsabilidade sempre que se ausentar de seu posto de trabalho.

5.1.2. Cabe aos gerentes de cada área:

5.1.2.1. Definir e controlar os privilégios de acesso de colaboradores e prestadores de serviço sob sua responsabilidade aos recursos de informática e às informações corporativas, conforme a necessidade do serviço;

5.1.2.2. Solicitar à ÁREA ADMINISTRATIVA que informe a ÁREA DE INFORMÁTICA, o bloqueio dos acessos lógicos que não se façam necessários aos usuários sob sua responsabilidade, e providenciar o bloqueio dos acessos físicos por meio de mecanismos de controle adequados;

5.1.2.3. Estabelecer mecanismos de supervisão de colaboradores ou prestadores de serviços sempre que estes venham a manipular direta ou indiretamente a informação sob a responsabilidade da sua área.

5.1.3. Cabe à ÁREA DE INFORMÁTICA:

5.1.3.1. Estabelecer mecanismos de controle lógico de acesso para proteção dos recursos computacionais e informações corporativas baseadas em computadores;

5.1.3.2. Adotar medidas de segurança, técnicas e administrativas aptas a proteger os 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.

5.1.3.3. Atender às solicitações dos gerentes de área em relação à criação e eliminação de contas de usuário e a concessão e exclusão de privilégios de acesso lógico aos recursos computacionais disponíveis;

5.1.3.4. Promover a segurança das senhas dos usuários, estabelecendo mecanismos para a rejeição de senhas de fácil adivinhação e para a exigência de troca da senha pelo usuário no mínimo a cada 90 dias.

5.1.4. Consiste em violação desta Política o uso de identificador de usuário e senha de outra pessoa para obtenção de acesso aos recursos de informática, assim como qualquer outra tentativa de obtenção de acesso físico ou lógico não autorizado a equipamentos, dados, documentos, sistemas e serviços de informação.

5.2. Uso de Hardware e Software.

5.2.1. É proibido:

5.2.1.1. Utilizar, nas dependências do Cibrius, equipamentos e softwares não homologados pela ÁREA DE INFORMÁTICA;

5.2.1.2. Instalar qualquer software, mesmo em caráter de demonstração, sem prévia autorização da ÁREA DE INFORMÁTICA;

5.2.1.3. Utilizar hardware ou software - inclusive espaço de armazenamento em disco e recursos de impressão - para finalidades pessoais ou não relacionadas às atividades de trabalho;

5.2.1.4. Trazer equipamentos próprios ou de terceiros para uso interno ou para serem consertados no ambiente do Cibrius;

5.2.1.5. Ingressar na sala de servidores do Cibrius sem a devida autorização por parte do Gerente da ÁREA DE INFORMÁTICA, a qual somente poderá ser concedida caso o acesso a essa dependência for necessário para alguma atividade de suporte, manutenção ou troca de equipamento, ou ainda para serviços de limpeza e conservação do local.

5.2.2. Cabe a cada usuário informar-se sobre o uso correto dos equipamentos e softwares utilizados e colaborar para a preservação da integridade e do bom funcionamento dos recursos de informática a ele confiados.

5.3. Uso de correio eletrônico e da Internet:

5.3.1. Os usuários dos serviços de correio eletrônico (e-mail) do Cibrius devem zelar pela sua utilização dentro dos princípios institucionais e pessoais constantes do Código de Ética, tendo em vista a preservação da imagem da Entidade.

5.3.2. O e-mail institucional, deve ser usado única e exclusivamente para assuntos profissionais.

5.3.3. Fica vedado o acesso a páginas da Internet de conteúdo pornográfico, de entretenimento e de assuntos de interesse pessoal não relacionado às atividades de trabalho.

5.3.4. O Acesso à Internet se dará entre as 08:00 e 18:00 initerruptamente, ficando a cargo do Diretor responsável pela área solicitante, as liberações que se façam necessárias.

5.4. Propriedade da informação:

5.4.1. Toda informação produzida e/ou mantida nos sistemas do Cibrius é de propriedade do Instituto e de responsabilidade da pessoa designada em cada caso como "gestor da informação".

5.4.2. Um gestor da informação será formalmente designado para os principais tipos de informações processadas (benefícios, investimentos, contabilidade etc.), correspondendo ao gestor sob cuja responsabilidade está a produção e/ou o tratamento da informação.

5.4.3. O gestor da informação é responsável por:

5.4.3.1. Garantir a integridade e a fidedignidade das informações registradas por sua equipe em sistemas de informação e relatórios;

5.4.3.2. Estabelecer as regras a serem aplicadas na concessão de privilégios de acesso para leitura/escrita de dados e informações aos diversos grupos de usuários; e

5.4.3.3. Identificar as informações a serem classificadas como sigilosas e submetê-las ao tratamento indicado no item 5.6.

5.4.4. A ÁREA DE INFORMÁTICA é responsável por identificar, implantar e manter os controles lógicos necessários a garantir o atendimento dos requisitos de segurança oriundos de especificações dos gestores da informação, de determinações da alta direção e dos resultados das análises de riscos efetuadas, tendo em vista o cumprimento desta Política.

5.5. Tratamento de Informações Confidenciais

5.5.1. São classificadas como confidenciais as informações que digam respeito a:

5.5.1.1. Dados pessoais armazenados em bases de dados corporativas, relativos a qualquer membro do Instituto, Participantes, Assistidos, Pensionistas ou de seus parceiros;

5.5.1.2. Senhas de acesso aos recursos computacionais;

5.5.1.3. Informações cuja revelação não-autorizada possa prejudicar pessoas ou comprometer planos, operações ou objetivos organizacionais, assim classificadas pela direção ou pelos gestores da informação.

5.5.2. Havendo necessidade de troca de informações confidenciais com partes externas, o mesmo só poderá ser feito, através de FTP (*File Transfer Protocol*), onde as informações são criptografadas, ou através de mecanismos, onde o acesso se dará através de senha (*OneDrive, google drive*, etc.), desde que em conformidade.

5.6. Preservação da continuidade do negócio

5.6.1. Tendo em vista a dependência do Cibrius em relação aos seus sistemas de informação para o adequado cumprimento de sua missão, devem ser adotadas as seguintes medidas para evitar a interrupção do acesso às informações e aos serviços de tecnologia da informação corporativos, cuja execução estará sob a responsabilidade da ÁREA DE INFORMÁTICA:

5.6.1.1. Sempre que constatado o risco de paralisação dos serviços de informática em decorrência de tentativa de invasão, ameaça de vírus, operação de usuário ou outra ameaça que coloque em risco o ambiente computacional da organização, devem ser adotadas as medidas cabíveis para conter os riscos, entre as quais poderá se incluir a interrupção temporária de um ou mais serviços de tecnologia da informação.

5.6.1.2. Nos casos em que for necessário interromper algum serviço, devem ser registrados pela ÁREA DE INFORMÁTICA os dados básicos sobre o incidente: data, hora, ameaça identificada, medidas adotadas para contê-la.

5.6.1.3. Os procedimentos de criação, teste e recuperação de backups (cópias-reserva de dados corporativos, configurações de sistemas e outras informações essenciais para a continuidade do negócio após a ocorrência de um desastre ou falha de hardware ou software) devem ser documentados e mantidos atualizados para assegurar a capacidade de recuperação dos serviços de tecnologia da informação da organização em caso de desastre.

5.6.1.4. Cópias-reserva dos dados críticos para a organização devem ser mantidas em localidade remota, para permitir sua recuperação em caso de perda ou indisponibilidade do backup mantido nas dependências da organização.

5.7. Aspectos Humanos da Segurança

5.7.1. Os usuários dos recursos de informação do Cibrius têm o direito ao acesso à informação necessária ao cumprimento desta Política de Segurança.

5.7.2. O processo de desligamento de empregado ou prestador de serviços do Cibrius deve incluir o bloqueio de todos os acessos aos sistemas do Instituto e o recolhimento dos equipamentos a ele confiados, além do disposto no item 5.1.2.2 (revogação dos privilégios de acesso lógico a ser solicitada à ÁREA DE INFORMÁTICA pelo gerente responsável).

5.8. Aquisição e Desenvolvimento de Software

5.8.1. A aquisição e o desenvolvimento de software no Cibrius estão sujeitos à observância dos seguintes princípios de segurança:

5.8.1.1. Princípio da Confidencialidade, que se caracteriza pela proteção da informação contra acessos não autorizados;

5.8.1.2. Princípio da Disponibilidade, consistindo na prevenção contra interrupções na operação de sistemas e no acesso à informação nos momentos em que houver necessidade.

5.8.1.3. Princípio da Integridade, que se traduz na proteção contra manipulações e alterações indevidas da informação;

5.8.1.4. Princípio da Autenticidade, que reflete a identificação daquele que produz, tem acesso à informação ou realiza qualquer operação que a utilize;

5.8.1.5. Princípio da Legalidade, que se conceitua como a produção, manipulação e guarda da informação em conformidade com preceitos legais;

5.8.1.6. Princípio da Auditabilidade, que significa a configuração de sistemas e bases de dados de forma a possibilitar o rastreamento de atividades físicas e lógicas;

5.8.1.7. Princípio da Integração, que define que os dados e informações da organização deverão constituir um conjunto harmônico e coerente, que reflita a integração sistêmica das áreas e funções corporativas;

5.8.1.8. Princípio da Eficácia, que visa a garantir que os sistemas atendem aos requisitos especificados e oferecem os resultados planejados.

5.8.2. A ÁREA DE INFORMÁTICA, em conjunto com o gestor da informação, deve estabelecer os requisitos a serem atendidos pelos sistemas e softwares aplicativos em processo de aquisição, bem como os procedimentos de teste a serem realizados para confirmar o atendimento dos requisitos antes de sua aprovação, a fim de garantir o máximo nível de conformidade possível com os princípios acima elencados.

5.9. Atividades de Auditoria e Administração do Risco

5.9.1. A ÁREA DE INFORMÁTICA é responsável por definir, implementar e manter documentados procedimentos voltados para:

5.9.1.1. A administração dos riscos, abrangendo, entre outras, as tarefas de monitoração da rede, atualização de antivírus, instalação de patches e atualização de versões de software, das configurações do firewall e de outros mecanismos de segurança;

5.9.1.2. A auditoria destinada tanto à avaliação periódica da segurança do ambiente computacional para fins preventivos quanto à investigação de incidentes após a sua detecção.

5.9.2. Os logs (registros cronológicos de atividades nos sistemas) e demais informações a serem usados para fins de auditoria devem ser objeto de tratamento especial, protegidos contra destruição e alteração indevida das informações por meio de mecanismos seguros de armazenamento e backup.

5.9.3. A qualquer momento e sem aviso prévio, o Comitê de Ética do Cibrius pode proceder ao exame dos arquivos armazenados nos computadores da organização, independentemente de sua natureza, e de apagar aqueles que contenham dados não condizentes com esta Política de Segurança.

6. DA COMPETÊNCIA

6.1. Cabe à Diretoria Executiva do Cibrius:

6.1.1. Aprovar as normas operacionais oriundas das diretrizes de segurança registradas nesta Política de Segurança da Informação, a serem elaborada pela área responsável por sua implementação; e

6.1.2. Prover os recursos necessários para o desenvolvimento das ações de segurança a cargo da ÁREA DE INFORMÁTICA e demais unidades executoras.

7. DAS PENALIDADES

7.1. A violação de disposição desta Política de Segurança sujeitará o infrator às sanções relacionadas no Código de Ética do Cibrius, bem como a outras estabelecidas por decisão da Diretoria Executiva.

8. DISPOSIÇÕES GERAIS

8.1. Esta Política está baseada também, nas melhores práticas do setor aplicadas ao assunto que se refere.

8.2. Os casos omissos serão analisados e decididos pela Diretoria Executiva.

9. DA VIGÊNCIA

9.1. Esta norma revoga a anterior de mesmo número e entra em vigor a partir da data de sua aprovação pelo Conselho Deliberativo.

APROVAÇÃO

11ª Reunião Ordinária do Conselho Deliberativo - Exercício 2020.

EM: 16/12/2020