POLÍTICA DE SEGURANÇA DE INFORMAÇÃO DO CENTRO BRASILEIRO DE ANÁLISE E PLANEJAMENTO (CEBRAP)

O objetivo desta política é proteger a confidencialidade, integridade e disponibilidade das informações acessadas ou produzidas pelo Cebrap, mantendo ativos e seguros os sistemas operacionais, as colaboradoras e colaboradores da instituição. Esta política é direcionada ao **público interno**, portanto, a colaboradores, efetivos ou temporários, e eventuais prestadores de serviço.

Este documento está organizado em duas partes, com objetivos específicos.

A primeira parte fornece uma base de conhecimento sobre questões fundamentais relacionadas aos diversos níveis de Segurança da Informação.

A segunda parte objetiva esclarecer as diretrizes relativas à Segurança da Informação dentro do Cebrap. Estas diretrizes buscam mitigar os riscos associados ao roubo, perda, mau uso, dano ou abuso dos sistemas de tecnologia da informação existentes e utilizados na casa ou pelos pesquisadores do Cebrap em suas atividades de pesquisa.

Vale ressaltar que, para efeitos de compreensão e destinação dos termos desta política, entende-se por “colaboradores” e “colaboradoras” todas as pessoas vinculadas a atividades de pesquisa ou projetos do Cebrap, bem como funcionários do quadro administrativo da instituição.

PARTE I: O QUE É UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO?

1. VISÃO GERAL DA POLÍTICA

Nesta seção são encontradas informações legais, baseadas nas normas técnicas de Segurança da Informação ABNT NBR ISSO/IEC 27002:2013, 0ABNT NBR ISO/IEC 27005:2019, ABNT NBR ISO/IEC, 31000:2018, associadas ao objetivo deste documento.

Informação é um ativo muito importante para as atividades da casa, uma vez que, para a execução de inúmeros projetos e pesquisas realizados pelo Cebrap, há coleta de dados pessoais de respondentes de *survey* ou entrevistados. Além disso, também existe captação e tratamento de dados fornecidos por colaboradores no momento de contratação e no desenvolvimento de trabalhos e prestação de serviços com a

instituição.

De acordo com a **Lei Geral de Proteção de Dados (LGPD)**, as organizações que tratam dados pessoais devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados, bem como de situações acidentais ou ilícitas que causem: destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

2. O QUE É SEGURANÇA DA INFORMAÇÃO?

Neste capítulo apresentamos alguns conceitos básicos sobre Segurança da Informação (SI), boas práticas e comportamentos a serem evitados.

Segurança da Informação é uma área de conhecimento dedicada à proteção de informações, que atua contra acessos não autorizados, alterações indevidas ou na indisponibilidade de sistemas.

A atuação dos profissionais especializados na área é balizada pelos seguintes princípios, que conformam os objetivos principais de sua atuação:

1. Confidencialidade, priorizando que as informações sejam tratadas apenas por pessoas autorizadas pelo Cebrap;
2. Integridade das informações, no sentido de que elas não sofram qualquer modificação indevida (de forma acidental ou não);
3. Disponibilidade constante das informações para as pessoas autorizadas a tratá-las.

Uma atuação responsável do ponto de vista da Segurança da Informação é pautada pela efetivação desses princípios. Desta forma, podem ser consideradas ameaças à SI quaisquer atos que ocasionam a perda, temporária ou permanente, de algum desses atributos, uma vez que isso pode impactar todos os processos que envolvem fluxo de informações no Cebrap.

Ameaças são agentes ou condições que comprometem a confidencialidade das informações. Elas interagem com as informações de forma direta, por meio da exploração de vulnerabilidades, que podem ser derivadas de *hardwares*, *softwares* ou comunicação humana.

Uma das consequências do vazamento de dados pessoais pode ser a inserção de códigos maliciosos no computador utilizado. Conhecidos como *malware*, esses códigos são utilizados para danificar o equipamento que eles adentram. Mas *malware* é um termo genérico, que inclui outros códigos maliciosos, como os *spyware*, utilizados para monitorar o uso e navegação do computador infectado, e mesmo para enviar as informações coletadas dessa maneira para terceiros. Também é possível citar o *adware*[1], projetado para apresentar propagandas direcionadas à pessoa que continua utilizando o equipamento.

Por outro lado, é importante ressaltar que a ocorrência de determinados fatos não implica um incidente de Segurança da Informação. Por exemplo, o envio incorreto de e-mail, que não contenha informações pessoais ou sigilosas, para terceiro desconhecido, não é uma falha de Segurança da Informação, assim como o compartilhamento de uma pasta com informações sigilosas entre áreas do Cebrap, considerando que ocorre dentro do ambiente virtual institucional (entre e-mails @cebrap).

PARTE II: DIRETRIZES E CONDUTAS ADOTADAS PELO CEBRAP

3. BOAS PRÁTICAS E O QUE EVITAR

Aqui destacamos algumas boas práticas adotadas pelo Cebrap com o objetivo de preservar as informações que estão nas bases de dados. A adesão às condutas previstas no capítulo a seguir é essencial para o bom funcionamento dos sistemas e, também, para evitar incidentes de privacidade e proteção de dados, pois qualquer falha pode gerar um impacto muito negativo à reputação do Cebrap e suas relações institucionais. Nesse sentido, o desrespeito às regras previstas nesta política pode gerar sanções, podendo inclusive justificar demissão, desligamento ou rescisão do contrato de prestação de serviços a depender da gravidade do desrespeito às condutas aqui previstas.

1) É proibida a utilização dos meios de transmissão eletrônica institucional (telefone, e-mail e outros) destinada ao desempenho das atividades profissionais, para o envio de mensagens:

- difamatórias, indecentes, obscenas ou de qualquer forma ofensivas a terceiros;
- que interfiram nas atividades normais do ambiente de trabalho;
- que importunam, de qualquer forma, uma outra pessoa;

[1] GORDON, S. Fighting Spyware and Adware in the Enterprise. EDPACS, v. 32, n. 12, p. 14–18, 1 jun. 2005.

- que tenham a intenção de enganar quanto à sua autoria ou sejam anônimas;
- que distribuam de forma ilícita *softwares* ou informações de terceiros protegidas por direitos autorais.

2) Não é permitido que pessoas sem autorização do Cebrap utilizem os serviços de telecomunicações ou mensagens eletrônicas fora do estabelecido nesta política.

3) Nunca deve ocorrer a duplicação de *softwares* adquiridos pelo Cebrap - ou de suas licenças -, salvo quando houver autorização expressa para tanto, nem deve ocorrer instalação de jogos ou *softwares* não oficiais nos equipamentos.

4) O servidor de arquivos local da instituição deve ser o meio primário de armazenamento de dados e *backup*, levando em consideração que, ao utilizar qualquer outro software ou equipamento não autorizado ao TI, é de plena responsabilidade do usuário a guarda e *backup* de tais dados.

5) É de responsabilidade de cada usuário o sigilo sobre as senhas de acesso – ou a qualquer sistema aplicativo acessível por meio dele – que a ele tenham sido confiadas.

6) Não é permitido editar documentos elaborados por outros usuários da rede sem a devida autorização, assim como não é permitido alterar informações de eventos e pastas compartilhadas sem consentimento.

7) Todo e qualquer material confiado para exibição, controle e atualização, sempre que solicitado, deve ser conservado pelo usuário, não sendo permitida cópia ou reprodução sem autorização expressa.

8) *Downloads* de programas ou arquivos de sites não autorizados pela área de TI devem ser realizados apenas quando imprescindível para a realização das atividades profissionais.

9) É vedada a utilização do servidor de arquivos local da instituição como meio de armazenamento de arquivos particulares.

10) Deve ser evitada a cópia ou utilização de arquivos de origem desconhecida ou duvidosa, recebidos por e-mail, celular ou outro tipo de mídia.

11) Não devem ser alteradas as configurações dos bens de informática ou de telecomunicações confiados ao usuário que possam expô-los a acessos indevidos, riscos desnecessários ou à contaminação por vírus de computador.

12) Os perfis de acesso dos sistemas da casa devem ser rigorosamente respeitados. O perfil administrador deve ser acessado somente por administradores de sistemas. O

perfil operacional deve ser definido de acordo com a atividade do colaborador e as pastas e *softwares* que ele pode ter acesso.

4. COMPETÊNCIAS E RESPONSABILIDADES SOBRE O USO DOS DADOS

A LGPD estipula a definição de "controlador de dados pessoais" e de "operador de dados pessoais"[2]*.*

Controlador de dados pessoais: o controlador é o agente responsável por tomar as principais decisões referentes ao tratamento de dados pessoais e por definir a finalidade deste tratamento. Entre essas decisões, incluem-se as instruções fornecidas a operadores contratados para a realização de um determinado tratamento de dados pessoais.

Operador de dados pessoais: o operador é o agente responsável por realizar o tratamento de dados em nome do controlador e conforme a finalidade por este delimitada.

Em atividades e rotinas científicas do Cebrap, o controlador de dados pessoais é o coordenador ou coordenadora de cada projeto. Em atividades e rotinas administrativas, o controlador de dados pessoais é a gerência administrativa e financeira.

4.1 A POSSIBILIDADE DE RESPONSABILIZAÇÃO DO CONTROLADOR E DO OPERADOR

Aqui detalhamos como ocorre a responsabilização por problemas ligados à Segurança da Informação.

Segundo a Lei Geral de Proteção de Dados, quando um tratamento é considerado irregular, ele também é ilícito, uma vez que pode derivar da falta de observação do controlador em relação à legislação e às medidas de segurança efetivas, considerando:

- o modo como o tratamento é realizado;
- o resultado e os riscos esperados do tratamento de dados;
- as técnicas de tratamento utilizadas.

Para que fique comprovado o dano, deve estar evidente quem é o prejudicado pela

[2] AGOSTINELLI, J. A importâancia da Lei Geral de Proteção de Dados Pessoais no ambiente online. ETIC - ISSN 21-76-8498, v. 14, n. 14, 24 set. 2018.

conduta, qual o dano causado pelo ato, e a ligação entre a conduta do agente de tratamento de dados e o dano gerado à vítima. O Cebrap poderá convidar outras instituições pertencentes à cadeia de tratamento de dados dentro da qual o dano foi causado para responder pelo dano, uma vez que a responsabilidade pelo dano é solidária, nos termos da legislação.

O controlador das informações é obrigado a reparar os possíveis danos derivados de sua conduta caso não consiga comprovar que:

- se realizou o tratamento necessário de dados pessoais;
- não se realizou o tratamento, mas não houve violação da legislação de proteção de dados; ou
- quando o dano for culpa exclusiva do titular de dados ou de terceiros.

5. ESTRUTURA INTERNA DE SEGURANÇA DA INFORMAÇÃO

A estrutura interna de segurança da Tecnologia da Informação (TI) do Cebrap é composta por diversos elementos e medidas que visam proteger os sistemas e as informações da instituição contra acessos não autorizados.

Para auxiliar nesta tarefa, o Cebrap conta com empresa especializada contratada, responsável pela administração e manutenção de todo o conjunto de tecnologia, incluindo computadores, servidores e aplicações. Além disso, a empresa de tecnologia contratada pelo Cebrap realiza análises de segurança para evitar quaisquer problemas com informações importantes, ameaças cibernéticas e outras vulnerabilidades.

Essa estrutura abrange as seguintes áreas:

Políticas de Segurança: Diretrizes estabelecidas pelo Cebrap para orientar as práticas de segurança da informação. Incluem aspectos como autenticação de usuários, controle de acesso, criptografia e regras de uso aceitável.

Gestão de Acessos: Processos para gerenciar identidades de usuários e controlar o acesso a sistemas e informações. Inclui criação de contas, atribuição de privilégios e monitoramento.

Proteção de Dados: Medidas para garantir a confidencialidade, integridade e disponibilidade dos dados. Envolve criptografia, *firewalls*, segurança de rede, detecção/prevenção de intrusões e *backups* regulares.

Gerenciamento de Vulnerabilidades: Identificação, avaliação e mitigação de vulnerabilidades em sistemas e infraestrutura de TI. Inclui aplicação de *patches* de segurança, testes de penetração, varreduras de vulnerabilidade e proteção contra *malware* e ataques cibernéticos.

Monitoramento e Resposta a Incidentes: uso de ferramentas de monitoramento em tempo real, análise de *logs*, detecção de incidentes e ações de resposta para minimizar danos e prevenir futuras ocorrências.

6. MEDIDAS TÉCNICAS E ADMINISTRATIVAS DE GARANTIA DA SEGURANÇA DA INFORMAÇÃO

Neste capítulo apresentamos os processos adotados pelas áreas responsáveis para garantir a proteção de dados e de contenção de danos, em casos de falhas.

6.1 MONITORAMENTO DOS NÍVEIS DE PROTEÇÃO DOS SISTEMAS

Todos os *logins* de entrada e saída do *firewall* e *file server* são monitorados, analisando essas interações a fim de observar as constantes tentativas de invasão dos sistemas da instituição. Também é feito um monitoramento crítico, em tempo real e com maior detalhamento, uma vez por semana, para compreender se aconteceram tentativas de invasão durante a semana e o seu grau de perigo.

Por meio do *firewall* é feito um monitoramento simplificado das práticas e atividades de acesso a páginas da internet pelos colaboradores. Vale ressaltar que, em relação aos colaboradores, não são monitoradas as interações nas páginas acessadas, **apenas o histórico de acesso a sites e plataformas**, respeitando-se a privacidade dos colaboradores da instituição.

6.1.1 COMO PROCEDEMOS EM CASO DE FALHAS DE SEGURANÇA

Dependendo do risco gerado pela falha de segurança identificada nos sistemas da instituição, são adotados procedimentos emergenciais. O nível de gravidade ocasionado pela falha de segurança identificada será diagnosticado mediante a análise do departamento de tecnologia do Cebrap, representado pela empresa de tecnologia contratada, que deverá ser comunicada pessoalmente, por e-mail, telefone ou Whats App.

Após a abertura da solicitação do atendimento e posterior análise do profissional responsável, será possível identificar qual foi a falha e a gravidade dos seus efeitos. Assim, os responsáveis pela Segurança da Informação decidem qual protocolo de ação será adotado para lidar com a situação.

Em se tratando de uma falha de segurança considerada menos crítica, como a perda de um *pen drive* no qual estavam armazenados dados não sensíveis, sugere-se reportar o ocorrido imediatamente à área Administrativa e aos responsáveis de T.I. para que as providências de segurança de dados sejam adotadas. Se o incidente se tratar de roubo ou furto de equipamentos, deve ser apresentado um Boletim de Ocorrência.

Nesse caso, se houver necessidade, as senhas do VPN e do *file server* podem ser trocadas mediante aviso ao usuário. No entanto, em caso de utilização externa do IP daquele usuário, ou seja, se uma pessoa de fora estiver acessando os sistemas do Cebrap, a senha é trocada **mesmo sem autorização do colaborador**.

Como medir a gravidade do incidente de segurança que pode ter ocorrido?

É importante considerar alguns aspectos:

- A quantidade de dados vazados: se houver o vazamento de uma quantidade muito grande de informações, mesmo que elas não sejam sensíveis, isso é considerado um incidente grave;

- O tipo de dado que foi acessado: quando se tratar de dados sensíveis como de saúde, sexualidade, gênero e raça, isso também é considerado um acidente grave;

- A possibilidade de identificação do caráter político do ataque à Segurança da Informação: por exemplo, o incidente ocorreu após uma aparição de um posicionamento de um pesquisador do Cebrap na grande mídia sobre um tema que tem implicações em interesses políticos de outros grupos; nesse sentido, o ataque pode ter sido feito para afetar ou atrapalhar o desenvolvimento normal de um projeto e/ou uma pesquisa.

Após a descoberta do incidente, mediante a gravidade, será formado um time composto pelo coordenador do projeto no qual o incidente ocorreu, pela pessoa do T.I, por uma pessoa do jurídico do Cebrap e por um membro da diretoria da instituição. Esse grupo irá trabalhar na produção de medidas e encaminhamentos para sanar eventuais problemas ocasionados pelo incidente.

6.2 ORIENTAÇÕES PARA A MANUTENÇÃO DA SEGURANÇA DE INFORMAÇÃO

Quando qualquer colaborador é contratado, a Gerência Administrativa requer o completo sigilo das informações que são disponibilizadas para o desenvolvimento do exercício profissional, inclusive após a rescisão de seu contrato. Além disso, é solicitado que não se utilize quaisquer informações, virtual ou pessoalmente, em benefício próprio ou de terceiros, sem expressa permissão.

Conta-se com a razoabilidade de todos os colaboradores para garantir a utilização responsável dos sistemas da instituição, usando-os somente para finalidades de interesse do Cebrap. Todas as informações presentes em tais sistemas devem ser consideradas confidenciais e colaboradores são responsáveis pelas condutas adotadas em quaisquer comunicações feitas em nome da instituição, sendo convidados sempre a tomar as devidas precauções, no sentido de evitar que terceiros façam uso da sua identificação de colaboradores de forma inapropriada.

Recomenda-se fortemente que coordenadores e coordenadoras de pesquisa (na figura de Controladores dos Dados) e Operadores (demais pesquisadores vinculados ao projeto) utilizem a estrutura Microsoft 365, em suas aplicações “One Drive” e “Share point”, sob o domínio “@cebrap.org.br”. Cada conta/e-mail neste domínio tem uma capacidade de armazenamento em nuvem de 1 TB. Após o término do projeto, recomenda-se a transferência para o servidor do Cebrap. Outra opção possível é o uso direto do servidor do Cebrap via acesso VPN. O não uso dessas estruturas implica a responsabilização direta do Controlador de Dados (coordenador do projeto) sobre eventuais quebras de segurança.

6.2.1 ORIENTAÇÕES PARA USO DE RECURSOS DE INFORMÁTICA

Ao usar os recursos de informática, os colaboradores estão cientes de que se responsabilizam pelo seu bom uso. Se comprometem também a atender o que dispõe a legislação em vigor, bem como o Código de Boas Práticas estabelecido dentro da instituição. Estar ciente pressupõe seguir as seguintes diretrizes aos colaboradores:

- assumir responsabilidade pelos equipamentos eletrônicos confiados aos colaboradores e disposição de zelar por eles;
- estar comprometidos a não receber ou fornecer componentes destes equipamentos ou, ainda, a mudança de sua localização, sem que a área responsável seja avisada;

- aceitar que o Cebrap é titular dos direitos de concessão do uso dos *softwares* ou da documentação objeto das licenças que lhe foram concedidas por terceiros: a reprodução do *software* ou da documentação sem permissão, além de ser infração contratual, sujeitará a pessoa (seja colaboradora ou não do Cebrap) às sanções de natureza civil e criminal, segundo estabelecem a Lei 7646/87 e os Códigos Civil e Penal brasileiros;

- proteger toda a informação acessada contra manipulação indevida, destruição e perda;

- zelar pela segurança e integridade dos dados pessoais, programas e equipamentos que fazem parte do escopo de suas atividades;

- manter a confidencialidade de todas as informações e dados do Cebrap e de seus associados, parceiros, colaboradores, mantenedores que utilizar, acessar ou processar;

- comunicar imediatamente à área de T.I. por meio de chamado em caso de suspeita de violação da segurança e proteção de dados, ou quaisquer outras irregularidades no acesso à rede, site, ou outros dispositivos técnicos.

6.2.2 ORIENTAÇÕES COMPARTILHAMENTO INTERNO DE DADOS

A leitura e ciência dos termos dessa Política implica assumir o compromisso de manter a confidencialidade de todos os dados e informações de propriedade do Cebrap, seus associados, financiadores, parceiros e colaboradores, respeitando a Lei Geral de Proteção de Dados e sua regulamentação, tomando as medidas necessárias para evitar:

- o acesso de pessoas não autorizadas aos arquivos e sistemas do Cebrap;
- a leitura, cópia, modificação ou remoção de dados sem autorização;
- a utilização ou inserção, nas redes institucionais, de arquivos ou dados eletrônicos, por meio de *pen drives*, e-mails ou qualquer outro meio não autorizado.

6.2.3 RECOMENDAÇÃO QUANTO AO DESLIGAMENTO DE COLABORADORES

Toda vez que houver o desligamento de colaboradores com acesso a sistemas internos (VPN, e-mail institucional, rede interna), por qualquer razão, **o(a) coordenador(a)** do núcleo/projeto ao qual a pessoa pertencia deve comunicar à **Gerência Administrativa e**

ao T.I., uma vez que será preciso desativar os acessos da pessoa aos sistemas e também ao e-mail institucional.

7. PROVEDORES DE SERVIÇOS UTILIZADOS PELO CEBRAP:

Aqui são listados os principais provedores de serviços utilizados para o armazenamento e segurança de informações do CEBRAP:

File server (Microsoft) - Solução robusta e escalável para armazenamento e compartilhamento de arquivos em redes locais, fornecendo recursos de gerenciamento avançados e segurança para garantir um acesso eficiente e seguro aos arquivos dentro de uma instituição.

Draytek Vigor 2927 - Possui recursos avançados de firewall, VPN e prevenção contra intrusões. Ele permite a criação de túneis VPN seguros para conexões remotas, garantindo que os dados sejam transmitidos de forma criptografada. Além disso, o roteador possui filtragem de conteúdo da web e recursos de controle de acesso para proteger a rede contra ameaças cibernéticas e garantir a conformidade com políticas de uso da Internet.

NAS (Backup) - Realiza cópias regulares dos dados do sistema, arquivos e pastas importantes. Isso garante que as informações críticas estejam protegidas contra perdas causadas por falhas de *hardware*, ataques de *malware*, erros humanos ou desastres naturais.

Microsoft 365 Business (Office e E-mails) - Solução abrangente baseada na nuvem, que oferece serviços e aplicativos essenciais para comunicação, colaboração e produtividade.

Microsoft Defender - Projetado para detectar e bloquear, *malware* como vírus, *trojans*, *ransomware* e *spyware* para proteger os dispositivos dos usuários.

Zabbix - Monitoramento (NOC - Network Operation Center) em tempo real, projetado para monitorar e rastrear o desempenho, a disponibilidade e a integridade de servidores, dispositivos de rede e outros recursos.