SERVIÇO GEOLÓGICO DO BRASIL
CPRM

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Tecnologia da Informação e Comunicação

Diretoria de Infraestrutura Geocientífica

Departamento de Informações Institucionais

Divisão de Informática

INFORMAÇÕES DOCUMENTAIS

Versão:	v1.0
Data de Criação:	quinta-feira, 25 de abril de 2019
Última Atualização:	sexta-feira, 1 de novembro de 2019
Nível de Segurança:	3 - Uso Interno
Autor:	Tiago Moura Evangelista

HISTÓRICO

Editor	Data	Comentários	Aprovado por	Versão
Tiago Moura Evangelista	25/04/2019	Versão Inicial	Ricardo Barcelos	v1.0

Companhia de Pesquisa de Recursos Minerais
Serviço Geológico do Brasil

ÍNDICE GERAL

1 APRESENTAÇÃO

Art. 1. A presente Política de Segurança da Informação vem estabelecer as diretrizes de uso e manutenção responsável dos dados, informações e conhecimentos pertencentes ao Serviço Geológico do Brasil – CPRM, visando sua segurança, preservação, proteção, continuidade e adequado desempenho.

§ 1º As definições presentes nesta política abrangem todos os usuários ou entidades que interajam com o ambiente informacional mantido pelo Serviço Geológico do Brasil – CPRM, independente do vínculo empregatício existente com a companhia.

§ 2º Todos os colaboradores do Serviço Geológico do Brasil – CPRM devem manter-se atualizados e obedientes às políticas em vigor.

§ 3º Os atos praticados em desconformidade com esta política serão de inteira responsabilidade dos colaboradores envolvidos, e sujeitos às sanções administrativas e penais cabíveis.

Art. 2. A tecnologia da informação e comunicação é um processo contínuo, portanto possíveis alterações nesta política serão implementadas sempre que necessário, refletindo as necessidades do Serviço Geológico do Brasil – CPRM e as evoluções tecnológicas do ambiente computacional.

Parágrafo Único. A publicação de uma nova versão desta Política Normativa, revoga automaticamente sua versão anterior.

2 FINALIDADE

Art. 3. A presente Política de Segurança tem por finalidade definir diretrizes claras e objetivas para a correta e adequada utilização e manutenção dos dados, informações e conhecimentos pertencentes ao Serviço Geológico do Brasil – CPRM, abrangendo todos as entidades e colaboradores envolvidos, focando em sua segurança, preservação, proteção, continuidade e adequado desempenho.

3 PÚBLICO ALVO

Art. 4. As normas aqui dispostas aplicam-se a todos os usuários do ambiente computacional e tecnológico oferecido e mantido pelo Serviço Geológico do Brasil – CPRM, independente de vínculo empregatício, e a quaisquer pessoas ou entidades que interajam com equipamentos e/ou serviços computacionais nele disponíveis.

4 ENTIDADES INSTITUCIONAIS

Art. 5. As seguintes entidades institucionais possuem importância finalística e determinante no âmbito desta Política Normativa:

I – Diretoria de Infraestrutura Geocientífica (DIG), entidade ligada diretamente à Presidência, responsável pelas estratégias e decisões de alto nível;

II – Departamento de Informações Institucionais (DEINF), entidade diretamente ligada a Diretoria supracitada, tem por objetivo básico a condução dos assuntos referentes às informações institucionais, cabendo-lhe especificamente o estudo, o planejamento, o controle, a coordenação e a implantação de técnicas voltadas para a captura, o armazenamento, o tratamento, a análise e a disseminação de informações do Serviço Geológico do Brasil – CPRM;

III – Divisão de Informática (DIINFO), entidade responsável diretamente pela estratégia, tomada de decisão e execução das atividades relacionadas à tecnologia da informação e comunicação. Atua nacionalmente junto a todas as Equipes de TI locais;

IV – Comitê Estratégico de Tecnologia da Informação e Comunicação (CETIC), formado por executivos de negócios e de tecnologia. Órgão colegiado responsável por promover a entrega de valor por meio da Tecnologia da Informação e Comunicação – TIC e do uso estratégico da informação na organização.

V – Comitê de Segurança da Informação (CSI), órgão colegiado de função consultiva e executiva. Estabelece os padrões e procedimentos relativos a segurança das informações e comunicações no âmbito do Serviço Geológico do Brasil – CPRM.

5 CONCEITUAÇÃO

Art. 6. Para os fins dispostos nesta Política Normativa aplica-se a seguinte conceituação técnica:

I – Ambiente Tecnológico. Todos os recursos, equipamentos, softwares e serviços mantidos e oferecidos aos colaboradores do Serviço Geológico do Brasil – CPRM. Também referido nesta norma como ambiente computacional ou infraestrutura tecnológica e demais sinônimos cabíveis.

II – Auditoria. Exame cuidadoso e sistemático das atividades desenvolvidas em determinada empresa, cujo objetivo é averiguar se elas estão de acordo com as planejadas e/ou estabelecidas previamente, se foram implementadas com eficácia e adequadas à consecução dos objetivos.

III – Autenticação. Ato de estabelecer ou confirmar algo como autêntico. Em um ambiente computacional refere-se a métodos e tecnologias de comprovação de identidade eletrônica: conjunto usuário/senha, biometria, meios físicos dentre outras tecnologias.

IV – Características Funcionais. Conjunto de aspectos e atributos que possibilitam definir quais as funções passíveis de realização por determinado equipamento.

V – Chamado. Método interno do Serviço Geológico do Brasil – CPRM para solicitação de serviços, reparos e demais atividades de suporte à Equipe de TI local.

VI – Colaborador. Toda pessoa ou entidade envolvida em atividades institucionais de interesse do Serviço Geológico do Brasil – CPRM,

colaborando assim para o desenvolvimento dos processos e objetivos desta organização.

VII – Credencial de Acesso. Conjunto usuário/senha utilizado como forma de autenticação dentro de um ambiente tecnológico qualquer.

VIII – Deny of Service (DoS). Tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga.

IX – Detentor. Colaborador que possua determinado equipamento ou recurso oferecido pela instituição atrelado ao seu nome, via de regra, através dos sistemas de controle patrimonial em corrente uso.

X – Dispositivos Móveis. Notebooks, smartphones, discos externos removíveis, tablets, GPSs

XI – Dispositivos Multiplicadores de Acesso. Todo e qualquer dispositivo que permita a conexão de mais de um equipamento a um único ponto de acesso a rede de dados da instituição. E.g. hubs, switches, roteadores, sejam eles com ou sem fio.

XII – Dynamic Host Configuration Protocol (DHCP). Protocolo utilizado em redes de computadores que permite a estes obterem um endereço IP automaticamente.

XIII – Grupo. Conjunto de usuários com as mesmas permissões e níveis de acesso aos recursos de rede. Grupos são utilizados visando racionalizar e agilizar a administração do ambiente computacional, agrupando usuários de mesmas caracteristicas.

XIV – Hibernação. Estado de economia de energia projetado principalmente para laptops. Enquanto a suspensão coloca seu trabalho e as configurações na memória e usa uma pequena quantidade de energia, a hibernação coloca no disco rígido os documentos e programas abertos e desliga o computador.

XV – Hoax. Mentira elaborada que tem como objetivo enganar pessoas.

XVI – Ilha de Impressão. Local onde concentram-se os equipamentos destinados a impressão de documentos.

XVII – Inventariar. Ato de relacionar, catalogar, lista, levantar a situação real de um conjunto de itens ou objetos pertencentes a uma organização.

XVIII – Lista de Distribuição. Agrupamento de usuários de mesma característica visando facilitar o envio de correspondência eletrônica.

XIX – Mail Bombing. Abuso que consiste em enviar grandes volumes de e - mail para um endereço na tentativa de estourar a caixa de correio, sobrecarregar o servidor onde o endereço de e-mail está hospedado, . ataque de serviço (ataque DoS), ou como uma cortina de fumaça para distrair a atenção de mensagens de e-mail importantes que indicam uma violação de segurança.

XX – Peer-to-Peer (P2P). Arquitetura de redes de computadores onde cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central.

XXI – Phishing. Técnica de fraude online utilizada por criminosos para roubar senhas de banco e demais informações pessoais, usando-as posteriormente de maneira fraudulenta.

XXII – Ponto de Acesso. Interface de conexão com a rede interna de dados e comunicações da instituição. Pode ter constituição física, como os pontos de conexão com a rede cabeada, bem como constituição imaterial, como no caso das redes sem fio.

XXIII – Powerlines. Equipamento de extensão de alcance de redes sem fio que se utilizam da rede elétrica comum para ampliar a abrangência e melhorar a qualidade do sinal.

XXIV – Privilégios de Administrador. Mais alto nível de privilégio possível que um usuário pode possuir como configuração de segurança de um equipamento computacional.

XXV – Proxy. Servidor que age como um intermediário para requisições de clientes solicitando recursos de outros servidores.

XXVI – Rede de Dados. Todo o ambiente e seus recursos e equipamentos responsáveis pela interconexão e comunicação dos fluxos de informação do Serviço Geológico do Brasil – CPRM.

XXVII – Service Level Agreements (SLA). Acordo de Nível de Serviço. Contrato entre duas partes: entidade prestadora de serviço e cliente beneficiário deste. Estão especificados, detalhadamente, todos os aspectos do tipo de serviço que será prestado, assim como os prazos contratuais e a qualidade do serviço.

XXVIII – Servidor de Arquivos. Equipamento disponibilizado para acesso dos usuários da rede do Serviço Geológico do Brasil – CPRM com o intuito de armazenar todos os documentos e mídias de cunho institucional.

XXIX – SPAM. Prática de envio em massa de e-mails não solicitados. As características principais são o envio da mensagem para milhares de pessoas ao mesmo tempo e a ausência de autorização do destinatário para utilização do seu endereço eletrônico.

XXX – Suspensão. Estado de economia de energia que permite que o computador reinicie rapidamente a operação em energia plena.

XXXI – Usuário. pessoas, entidades ou organizações que façam uso de determinado recurso ou serviço computacional. Também nominados como utilizador ou colaborador no âmbito desta Política Normativa.

6 DISPOSIÇÕES GERAIS

Art. 8. Todos os usuários que com acesso aos dados, informações e conhecimentos disponíveis através dos recursos computacionais, de rede, comunicação e informação deverão assinar os termos de "**Conhecimento**", "**Uso e Responsabilidade**" e "**Sigilo e Confidencialidade**" disponíveis em anexo à Política Normativa.

§ 1º Nos termos supracitados o usuário se compromete à estrita observância e obediência às normas de uso dos recursos computacionais e tecnológicos e políticas de segurança do Serviço Geológico do Brasil – CPRM.

§ 2º Seu descumprimento incorrerá nas penalidades cabíveis, de acordo com a infração cometida e com a legislação vigente.

§ 3º Os referidos termos deverão estar disponíveis para download na intranet do Serviço Geológico do Brasil – CPRM.

Art. 9. As políticas aqui elencadas trazem, como premissa básica, o conceito de que tudo o que não for explicitamente permitido é considerado violação à corrente Política de Segurança.

Art. 10. Cabe ao usuário, como detentor nos termos desta política, garantir a segurança das informações sob sua guarda, armazenadas localmente como computadores, notebooks, discos externos removíveis, pendrives e demais dispositivos portáteis.

Art. 11. Esta política deve ser amplamente divulgada e disponibilizada entre todos os colaboradores que atuem nesta organização e que possuam qualquer tipo de envolvimento com o ambiente computacional objeto desta Política de Segurança.

Art. 12. Em nenhuma hipótese será permitido o descumprimento desta política

Art. 13. O Serviço Geológico do Brasil – CPRM se exime das responsabilidades decorrentes da violação de qualquer um dos itens desta política.

§ 1º Fica o colaborador responsável pelos atos ilícitos ou danosos, praticados utilizando os recursos computacionais desta organização, que venham a causar prejuízos ou ônus às informações, sistemas, imagem, equipamentos ou terceiros.

§ 2º Os colaboradores devem estar cientes de que as informações, dados e conhecimentos gerados e manuseados a partir dos sistemas do Serviço Geológico do Brasil – CPRM são de propriedade única e exclusiva desta instituição.

Art. 14. O descumprimento das disposições constantes nessa política caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil.

Art. 15. A presente Política de Segurança entrará em vigor após sua deliberação pela Diretoria Executiva e sua publicação nos devidos meios de comunicação oficiais.

Art. 16. Os casos omissos nesta Política de Segurança serão dirimidos pelo Chefe da Divisão de Informática - DIINFO, ouvidas, quando for o caso, as devidas instâncias superiores.

7 BIBLIOGRAFIA

1 ADMINISTRADORES.COM.BR. Políticas de uso dos computadores. **Administradores**, Janeiro 2015. Disponivel em: <https://administradores.com.br/artigos/politicas-de-uso-dos-computadores>. Acesso em: 06 maio 2019.

2 SISP - SISTEMA DE ADMINISTRAÇÃO DE RECURSOS DE TECNOLOGIA DA INFORMAÇÃO. **Guia de Comitê de TI do SISP**. Brasil. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Logística e Tecnologia da Informação.. Brasília, p. 58. 2013. (CDU 658.011.56).

3 STI/COTEC. **Política de utilização de Recursos de TI**. CJF - Conselho da Justiça Federal. Brasília, p. 13. 2013.

4 DIRETORIA DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO. **Regulamento de Gestão e de Utilização de Recursos de Tecnologia da Informação da UTFPR**. Universidade Tecnológica Federal do Paraná. Curitiba, p. 13. 2013.

5 ASSOCIAÇÃO NACIONAL DOS SERVIDORES DA JUSTIÇA DO TRABALHO - ANAJUSTRA. **Política de uso dos Recursos Computacionais**. Associação Nacional dos Servidores da Justiça do Trabalho - ANAJUSTRA. Brasília, p. 9. 2011.

6 SECRETARIA DE ESTADO DE INFRAESTRUTURA E LOGÍSTICA – SINFRA. **Política Sobre Regras Gerais de Uso de Ativos de TI (Software e Hardware) – os programas, a rede de computadores, de dispositivos portáteis e de demais recursos de tecnologia da informação da Secretaria de Estado de Infraestrura e Logística – SINFRA.** Secretaria de Estado de Infraestrura e Logística – SINFRA. Cuiabá, p. 17. 2017.

7 INSTITUTO FEDERAL CATARINENSE – CAMPUS SÃO FRANCISCO DO SUL. **Política Para Utilização De Ativos De Informática E Acesso À Rede Do Instituto Federal Catarinense Campus São Francisco Do Sul**. Instituto Federal Catarinense. São Franscisco do Sul, p. 8. 2016.

8 TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO. **Portaria Nº 4.772**. Tribunal Regional do Trabalho da 4ª Região. Porto Alegre, p. 74. 2008.

9 DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES. **Uso de Dispositivos Móveis nos aspectos relativos à Segurança da Informação e Comunicações nos orgãos e entidades da Administração Pública Federal**. Gabinete de Segurança Institucional da Presidência da República. Brasília, p. 5. 2012.

10 SGB - SERVIÇO GEOLÓGICO DO BRASIL. Estrutura Organizacional. **CPRM - Serviço Geológico do Brasil**, 2018. Disponivel em: <http://www.cprm.gov.br/publique/media/sobre/organograma_2018.pdf>. Acesso em: 06 maio 2019.

11 CONSELHO FEDERAL DE MEDICINA VETERINÁRIA. Implantação da Política de Impressão. **Conselho Federal de Medicina Veterinária**, 15 Outubro 2018. Disponivel em: <http://portal.cfmv.gov.br/lei/download-arquivo/id/1085>. Acesso em: 19 jun. 2019.

12 TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO. Portaria GP n. 1260. **Tribunal Regional do Trabalho da 14ª Região**, 11 Julho 2017. Disponivel em: <http://www.trt14.jus.br/documents/10157/b3dff092-8032-475b-9114-42b812b92dde>. Acesso em: 19 jun. 2019.

13 EBSERH - EMPRESA BRASILEIRA DE SERVIÇOS HOSPITALARES. Política De Armazenamento de Arquivos Digitais. **Empresa Brasileira de Serviços Hospitalares**, 13 maio 2016. Disponivel em: <http://www2.ebserh.gov.br/documents/16692/1227758/Anexo+Resolu%C3%A7%C3%A3o+41+-SGPTI-Pol%C3%ADtica_de_armazenamento_de_arquivos+%281%29.pdf/d11d85b9-82ff-4c39-9e40-780c464cd488>. Acesso em: 25 jun. 2019.

14 BRASIL. Decreto Nº 9.637, De 26 De Dezembro De 2018. **Política Nacional de Segurança da Informação - PNSI**, Brasilia, DF, 26 Dezembro 2018. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm>. Acesso em: 26 jun. 2019.

15 TCU - TRIBUNAL DE CONTAS DA UNIÃO. Boas Práticas em Segurança da Informação, 2012. Disponivel em: <http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf>. Acesso em: 27 jun. 2019.

ANEXO I – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Art. 1. É objetivo finalístico desta Política Normativa de Segurança da Informação e Comunicação assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações e conhecimentos peculiares ao Serviço Geológico do Brasil – CPRM.

Art. 2. É proibida a divulgação de informações confidenciais do Serviço Geológico do Brasil – CPRM em grupos de discussão, listas, bate-papo, sites externos ou qualquer outro meio de comunicação, não importando se a divulgação foi deliberada ou inadvertida.

§ 1º A transferência de arquivos para colaboradores ou interessados externos à rede do Serviço Geológico do Brasil – CPRM cujo tamanho exceda a possibilidade de envio pelo e-mail institucional ou demais ferramentas corporativas, deverá ser realizada através da solução FileSender da RNP, mecanismo de confiabilidade e segurança atestados.

§ 2º O parágrafo anterior refere-se a usuários que estejam impossibilitados de acessarem a rede interna. Todas as demais transferências, independentemente de tamanhos e espécies de arquivo, deverão ser realizadas via servidor de arquivos ou rede interna entre os computadores dos colaboradores interessados.

Art. 3. Todos os colaboradores do Serviço Geológico do Brasil – CPRM que executem oficialmente atividades corporativas vinculadas a esta instituição devem assinar o "**Termo de Confidencialidade e Sigilo"** quanto ao sigilo de dados, informação e conhecimentos.

Art. 4. Todos os usuários devem ser conscientizados e treinados nos procedimentos de segurança da informação.

Art. 5. Quando do afastamento, mudança de responsabilidades, lotação ou atribuições dentro da organização, se faz necessária a revisão imediata dos direitos de acesso e uso de recursos.

Art. 6. Quando da efetivação do desligamento de usuário, deverão ser extintos todos os direitos de acesso e uso dos ativos a ele atribuído.

Art. 7. Todo ativo produzido pelo usuário desligado deverá ser mantido pela Serviço Geológico do Brasil – CPRM, garantindo o reconhecimento e o esclarecimento da propriedade do acervo para instituição.

Art. 8. Incumbe à chefia imediata solicitar à Equipe de TI local:

I – Os acessos necessários ao desenvolvimento das atividades dos colaboradores sob sua competência;

II – A alteração dos níveis de acesso ou a remoção do acesso a sistemas concedidos aos colaboradores, sempre que necessária sua adequação às atividades desenvolvidas;

III – A remoção dos acessos concedidos aos colaboradores, imediatamente após o afastamento ou desligamento da instituição.

Parágrafo Único. Não solicitada a alteração ou exclusão no momento oportuno, a chefia poderá ser responsabilizada pelo acesso indevido do colaborador a informações da instituição.

Art. 9. O privilégio de administrador na estação de trabalho é restrito aos membros da Equipe de TI local que necessitem de acesso privilegiado para o desempenho das atividades funcionais.

Parágrafo Único. A concessão de privilégio de administrador local será realizado conforme estabelecido no **Erro! Fonte de referência não encontrada.** do **Erro! Fonte de referência não encontrada.**.

Art. 10. O acesso privilegiado aos sistemas e serviços de TIC serão concedidos aos membros da Equipe de TI local sempre que necessários ao desempenho das atividades funcionais, de modo a permitir gerenciamento do ambiente tecnológico.

Art. 11. Na utilização das credenciais de acesso, compete ao usuário observar os procedimentos a seguir indicados, bem como adotar outras medidas de segurança de caráter pessoal, com vista a impedir o uso não autorizado do ambiente tecnológico a partir de sua conta de acesso:

I – Não compartilhar a senha com outras pessoas;

II – Não armazenar senhas em local acessível por terceiros;

III – Não utilizar senhas de fácil dedução como as que contém nomes próprios e de familiares, datas festivas e/ou sequências numéricas;

IV – Ao ausentar-se de sua estação de trabalho, ainda que temporariamente, o usuário deverá encerrar ou bloquear a sessão.

Art. 12. A senha deverá satisfazer os seguintes requisitos de complexidade:

I – Não conter nome da conta do usuário (login) ou mais de XXX caracteres consecutivos de partes de seu nome completo;

II – Possuir no mínimo 8 caracteres;

III – Conter caracteres de, no mínimo, três das quatro categorias a seguir:

(1) Caracteres maiúsculos (A-Z);

(2) Caracteres minúsculos (a-z);

(3) Dígitos de base (0 a 9);

(4) Caracteres não alfabéticos (e.g. !, @, #, $, %, ¨, &, *, -, _, +, = ...).

IV – Não coincidir com as últimas 05 senhas previamente utilizadas;

Parágrafo Único. A senha das credenciais de acesso de cada usuário deverá ser alterada a cada 180 dias.

Art. 13. Em caso de suspeita de comprometimento da senha ou de outro recurso de autenticação, o usuário comunicará imediatamente à Equipe de TI local que poderá, como medida preventiva, suspender temporariamente o acesso.

Art. 14. O usuário é o único e exclusivo responsável pelas atividades realizadas por meio da utilização de suas credenciais de acesso ao ambiente computacional do Serviço Geológico do Brasil – CPRM.

Art. 15. As situações abaixo identificadas acarretam a suspensão das credenciais de acesso do usuário envolvido:

I – Conta com 05 tentativas sucessivas de autenticação com senha incorreta;

II – Conta sem uso por período igual ou superior a 90 dias;

§ 1º A suspensão de conta a que se referem os incisos I e II deverá ser realizada automaticamente.

§ 2º A suspensão de conta pode ser revogada pela Equipe de TI local mediante solicitação do usuário.

Art. 16. A suspensão e a posterior reativação das credenciais de acesso para a hipótese prevista no Art. 15 são realizadas pela Equipe de TI local a partir de solicitação encaminhada pela área de Gestão de Pessoas.Cabe a área de Gestão de Pessoas informar a Equipe de TI local quando dos afastamentos, licenças, desligamento ou quaisquer eventos que modifique o status de um colaborador quanto ao seu acesso as redes de comunicação do Serviço Geológico do Brasil – CPRM.

Art. 18. A alteração da senha associada às credenciais de acesso do usuário deve ser efetuada pelo próprio usuário.

Parágrafo Único. Quando da impossibilidade da realização da ação descrita no caput, a chefia imediata pode solicitar à Equipe de TI local que a execute.

Art. 19. O acesso físico ao CPD – Central de Processamento de Dados deve ser restrito à Equipe de TI local.

Paragráfo Único. Somente com autorização e presença de algum membro desta equipe será permitido o acesso ou a visitação da área.

Art. 20. Todos os CPD's do Serviço Geológico do Brasil – CPRM devem possuir a seguinte estrutura:

I – Espaço fechado e dedicado para os equipamentos de core, como storages, servidores, switches, no-breaks e demais equipamentos presentes na unidade;

II – Ar-condicionado dedicado e exclusivo, mantido em operação em regime 24/7 e em sua temperatura mínima;

III – Alguma área que possibilite acesso visual interno, área envidraçada, janela na parede ou na porta;

IV – Porta com fechadura eletrônica de acesso através de senha e biometria;

V – Medidores de temperatura e humidade monitoráveis e com alguma forma de visualização das medições;

VI – Grupo gerador independente capaz de sustentar toda a operação do CPD por XXX horas.

Art. 21. A informação utilizada pelo Serviço Geológico do Brasil – CPRM é um bem detentor de valor e importância. Ela deve ser protegida e gerenciada adequadamente com o objetivo de garantir a sua disponibilidade, integridade, confidencialidade, autenticidade e auditabilidade, independente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado.

Art. 22. Cada usuário deve acessar apenas as informações e os ambientes previamente autorizados. Qualquer tentativa de acesso a ambientes não autorizados será considerada uma violação dessa Norma.

Art. 23. A destruição de dados sigilosos deve ser feita por método que sobrescreva as informações armazenadas. Se não estiver ao alcance do órgão a destruição lógica, deverá ser providenciada a destruição física dos dispositivos de armazenamento.

ANOTAÇÕES

ANOTAÇÕES