MINISTÉRIO DA INTEGRAÇÃO E DO DESENVOLVIMENTO REGIONAL
SUPERINTENDÊNCIA DO DESENVOLVIMENTO DA AMAZÔNIA

ANEXO I

NORMA DE CONTROLE DE ACESSO LÓGICO

CAPÍTULO I

DO OBJETIVO

Art. 1º Esta norma, complementar à Política de Segurança da Informação e Comunicações – POSIC da Superintendência do Desenvolvimento da Amazônia - Sudam, tem por finalidade estabelecer diretrizes para implementação de controles de acesso lógico relativos à segurança da informação no âmbito da Sudam.

Parágrafo único. Esta norma não abrange o controle de acesso físico aos ativos de tecnologia da informação.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 2º Para os fins desta norma complementar, considera-se:

I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

II - arquivos: agrupamento de registros que, geralmente, seguem uma regra estrutural e que possuem informações (dados);

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

IV - autenticação de multifatores (MFA): utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema . Os fatores de autenticação se dividem em: algo que o usuário conhece (senhas, frases de segurança, PIN, dentre outros); algo que o usuário possui (certificado digital, **tokens**, códigos enviados por SMS, dentre outros); algo que o usuário é (aferível por meios biométricos, tais como digitais, padrões de retina, reconhecimento facial, dentre outros); e onde o usuário está (quando o acesso só pode ser feito em uma máquina específica, cujo acesso é restrito);

V - autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

VI - confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, sistema, órgão ou entidade não autorizado ou não credenciado;

VII - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

VIII - credenciais ou conta de acesso: permissão concedida por autoridade competente, após o processo de credenciamento, que habilita determinada pessoa, sistema ou organização ao acesso ao ambiente físico ou lógico. A credencial pode ser física, como crachá, cartão e selo, ou lógica, como identificação de usuário e senha ou dispositivo digital (**token**);

IX - criptografia: arte de proteção da informação, por meio de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem;

X - disponibilidade: propriedade que garante que informações e serviços estejam acessíveis e utilizáveis sob demanda por pessoas, sistemas, órgãos ou entidades, devidamente autorizados;

XI - gestão de riscos de segurança da informação: conjunto de processos que permitem identificar, analisar, avaliar e implementar medidas de proteção necessárias para o tratamento de riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

XII - integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XIII - prestador de serviço: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderá receber credencial especial de acesso;

XIV - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações;

XV - recursos de TIC: todo equipamento ou dispositivo que utiliza tecnologia da informação, bem como qualquer recurso ou informação que seja acessível por meio desses equipamentos ou dispositivos tecnológicos, tais como impressoras, sistemas, programas, softwares, acessos à rede local, internet, VPN (rede particular virtual), **pendrives**, **smartcards**, **tokens**, **smartphones**, modems sem fio, **desktops**, pastas compartilhadas em rede, entre outros;

XVI - rede local: conjunto de recursos compartilhados por meio dos servidores de rede, cabeamento estruturado, **switches**, pontos de acesso sem fio e dispositivos clientes, por onde trafegam as informações corporativas da Sudam;

XVII - rede sem fio (**wireless**): sistema que interliga dispositivos utilizando o ar atmosférico como via de transmissão por meio de ondas eletromagnéticas;

XVIII - sistema de informação: aplicação da Tecnologia da Informação que dá apoio às atividades de determinada área de conhecimento, visando otimizar as operações, o gerenciamento e a decisão, trabalhando os dados e transformando-os em informação;

XIX - termo de responsabilidade: termo assinado pelo usuário concordando em contribuir com a disponibilidade, integridade, confidencialidade e autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

XX - tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

XXI - unidade organizacional: elemento básico da estrutura hierárquica onde são lotados os usuários de uma organização;

XXII - usuários: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação da Sudam, formalizada por meio da assinatura do Termo de Responsabilidade; e

XXIII - webconferência: reunião ou encontro virtual realizado pela internet por meio de aplicativos ou serviço com possibilidade de compartilhamento de apresentações, voz, vídeos, textos e arquivos por meio da web.

CAPÍTULO III

DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 3º Esta norma complementar à POSIC/Sudam está fundamentada, sem prejuízo de outras legislações aplicáveis, nos seguintes normativos:

I - Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);

II - Decreto nº 9.573, de 22 de novembro de 2018, que Aprova a Política Nacional de Segurança de Infraestruturas Críticas;

III - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

IV - Decreto nº 10.046, de 09 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal;

V - Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

VI - Decreto nº 10.332, de 28 de abril de 2020, que institui a Estratégia de Governo Digital para o período de 2020 a 2023;

VII - Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal;

VIII - Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação;

IX - Portaria SGD/MGI nº 852, de 28 de março de 2023, que dispõe sobre o Programa de Privacidade e Segurança da Informação – PPSI;

X - Norma NBR ISO/IEC 27002:2013 - Código de Práticas para a Gestão da Segurança da Informação; e

XI - Guia do Framework de Privacidade e Segurança da Informação, versão 1.1.1, de junho de 2023, do Ministério da Gestão e da Inovação em Serviços Públicos.

CAPÍTULO IV

DAS DISPOSIÇÕES GERAIS

Art. 4º Esta norma complementar está alinhada às diretrizes gerais da Política de Segurança da Informação e Comunicações – POSIC da Sudam.

Parágrafo único. O objetivo precípuo desta norma é sistematizar a concessão de acesso lógico aos recursos de Tecnologia da Informação e Comunicações no âmbito da Sudam, a fim de evitar a quebra de segurança da informação.

Art. 5º A atualização deste documento é de responsabilidade do Comitê de Segurança da Informação e Comunicações.

Art. 6º O acesso às informações classificadas como públicas e de uso interno não é restringido com controles de acesso que discriminam o usuário.

Art. 7º O acesso às informações confidenciais e restritas serão permitidas apenas quando uma necessidade de trabalho for identificada e tal acesso aprovado pela Unidade Organizacional responsável.

Art. 8º O acesso a alguns equipamentos de hardware e/ou software especiais (tais como **firewall**, servidores de rede e bancos de dados, entre outros) é restrito aos servidores da Coordenação-Geral de Tecnologia da Informação e Comunicações.

Art. 9º A identificação, a autorização, a autenticação, o interesse do serviço e a necessidade de uso são condicionantes prévias para concessão de acesso aos recursos de Tecnologia da Informação da Sudam.

Art. 10. A identificação dos controles de acesso lógico, na Sudam, é consequência do processo de Gestão de Riscos de Segurança da Informação e Comunicações;

Art. 11. O acesso lógico aos recursos de Tecnologia da Informação da Sudam deve ser realizado por meio de sistema de controle de acesso.

§ 1º O acesso de que trata o caput deve ser concedido e mantido pela Divisão de Infraestrutura Tecnológica, baseado nas responsabilidades e tarefas de cada usuário;

§ 2º Terão direito ao acesso lógico à rede local, aos sistemas informatizados e aos serviços de TIC os usuários de recursos de tecnologia da informação.

§ 3º O acesso remoto deve ser realizado por meio de VPN - Rede Virtual Privada, após as devidas autorizações, devendo ser utilizado, preferencialmente, o MFA (**Multi-Factor Authentication** ou autenticação multifator) para a autenticação de acesso remoto.

Art. 12. A Divisão de Infraestrutura Tecnológica deve estabelecer e manter um inventário de todas as contas gerenciadas, no qual inclua contas de usuário, administrativas, testes e serviço.

Art. 13. A Divisão de Infraestrutura Tecnológica deve implementar a centralização da gestão de contas e do controle de acesso para todos os ativos de informação do órgão por meio de serviço de diretório e/ou provedor de SSO.

Art. 14. Para utilização dos recursos de Tecnologia da Informação da Sudam será obrigatório o uso de uma conta de acesso única, composta pelo nome de usuário (**login**) e senha de acesso, fornecidos pela Coordenação-Geral de Tecnologia da Informação e Comunicações, mediante solicitação formal da unidade requisitante.

CAPÍTULO V

DAS CONTAS DE ACESSO

Seção I
Do Cadastramento de Usuários

Art. 15. A criação de novas contas de acesso à rede e aos recursos de Tecnologia da Informação da Sudam se dará da seguinte forma:

I - para servidores e estagiários: através da abertura de chamado pela Coordenação-Geral de Pessoal, via Sistema GLPI, imediatamente após satisfeitas as condições de investidura e/ou admissão, informando os dados do usuário e anexando a documentação necessária;

II - para prestadores de serviço: após a abertura de chamado pelo Gestor do Contrato, via Sistema GLPI, imediatamente após satisfeitas as condições de ocupação do posto de trabalho, informando os dados do usuário e anexando a documentação necessária; e

III - para órgãos ou entidades que atuam na sede da Sudam: através da abertura de chamado pelo Gabinete da Sudam, via Sistema GLPI, após solicitação formal do órgão ou entidade requisitante, informando os dados funcionais do usuário.

Art. 16. As contas dos estagiários e prestadores de serviço serão configuradas para expiração automática ao fim da vigência do contrato.

Art. 17. Quando houver remoção do usuário para outra unidade ou o usuário passar a ocupar uma nova função, as permissões de acesso aos recursos de TIC devem ser revogadas.

§ 1º O novo superior imediato deve realizar a solicitação de novas permissões de acesso de acordo com a nova unidade/função do usuário.

§ 2º As permissões de acesso antigas devem ser imediatamente canceladas, conforme solicitação do antigo superior imediato.

Art. 18. Todos os usuários que utilizam ativos de informação da Sudam devem assinar o Termo de Responsabilidade sobre o uso de tais recursos.

Parágrafo único. A assinatura do Termo de Responsabilidade indica que o usuário em questão entende e concorda com as políticas, padrões, normas e procedimentos da Sudam relacionados ao ambiente de TIC, incluindo as instruções contidas nesta Norma, bem como as implicações legais decorrentes do não cumprimento do disposto nela.

Art. 19. As novas contas de acesso à rede e recursos de Tecnologia da Informação serão compostas por nome e sobrenome, sendo a forma padrão o nome e o último sobrenome, separados por ponto.

Parágrafo único. Caso a forma padrão incorra em homonímia com conta já existente, a Divisão de Infraestrutura Tecnológica realizará outra combinação a partir do nome completo do usuário para o qual a conta está sendo criada.

Art. 20. No ato da criação de conta de acesso à rede local, será automaticamente criada conta de acesso aos demais recursos de Tecnologia da Informação, de acordo com o perfil do usuário.

Parágrafo único. As permissões de acesso dos usuários à rede local e aos demais recursos de Tecnologia da Informação devem ser definidos pela unidade requisitante ao qual o usuário está vinculado, limitando-se às atividades estritamente necessárias à realização de suas tarefas.

Art. 21. As credenciais da conta de acesso (**login** e senha) são de uso pessoal e intransferível, sendo proibida a sua divulgação, empréstimo ou compartilhamento, sob pena de bloqueio pela Divisão de Infraestrutura Tecnológica quando constatada qualquer irregularidade.

Parágrafo único. Para retomar o acesso à rede, deverá ser formalizada nova requisição pelo titular da unidade do requisitante, via Sistema GLPI.

Seção II

Da Política de Senhas

Art. 22. A identificação de usuários que acessam a rede local e recursos de Tecnologia da Informação da Sudam deve ser feita mediante a autenticação usuário-senha, sendo a senha cadastrada um ativo de informação pessoal, intransferível e confidencial.

Art. 23. O padrão adotado para o formato da senha de acesso considera o tamanho mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores.

§ 1º A formação da senha de acesso deve seguir as seguintes regras:

I - as senhas associadas a contas gerais de usuários serão compostas utilizando uma quantidade mínima de 08 (oito) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais;

II - as senhas associadas a contas que possuem privilégio administrativo serão compostas utilizando uma quantidade mínima de 15 (quinze) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais;

III - não devem ser utilizados dados pessoais como nomes, sobrenomes, nomes de familiares ou de colegas de trabalho e informações de fácil obtenção como, por exemplo, placa do carro, data de aniversário ou endereço;

IV - não é permitida a repetição ou sequência de caracteres, números ou letras;

V - não deve ser utilizada qualquer parte ou variação do nome da Superintendência do Desenvolvimento da Amazônia - Sudam;

VI - não deve ser utilizada qualquer variação dos itens descritos acima como duplicação ou escrita invertida;

VII - não devem ser utilizados termos óbvios, tais como: “Brasil”, “senha”, “usuario’, “**password**” ou “**system**”; e

VIII - não devem ser reutilizadas as últimas 05 (cinco) senhas alteradas.

§ 2º A Divisão de Infraestrutura Tecnológica fornecerá inicialmente uma senha temporária para cada nova conta de acesso criada, devendo esta ser alterada pelo usuário quando do primeiro acesso à rede local.

Art. 24. As senhas de acesso serão renovadas obrigatoriamente a cada 180 (cento e oitenta) dias, devendo o usuário ser informado antecipadamente, via e-mail, para que proceda a mudança.

§ 1º Caso não seja efetuada a alteração da senha no prazo estabelecido, a conta de acesso será bloqueada até que a nova senha seja configurada.

§ 2º Em caso de suspeita de exposição indevida do ambiente de TIC, todas as senhas de acesso devem ser imediatamente alteradas.

§ 3º Em caso de comprometimento comprovado de segurança do ambiente de TIC por algum evento não previsto, todas as senhas de acesso deverão ser modificadas.

Seção III

Do Bloqueio, Desbloqueio e Cancelamento da Conta de Acesso

Art. 25. A conta de acesso será bloqueada nos seguintes casos:

I - após 5 (cinco) tentativas consecutivas de acesso incorreto;

II - solicitação do superior imediato do usuário, com a devida justificativa;

III - quando da suspeita de mau uso dos recursos de TIC disponibilizados pela Sudam ou descumprimento da Política de Segurança da Informação e Comunicações – POSIC e normas correlatas em vigência;

IV - após decorridos 45 (quarenta e cinco) dias consecutivos sem movimentação pelo usuário;

IV – após decorridos 30 (trinta) dias consecutivos quando do afastamento temporário do usuário servidor da Sudam, de acordo com as hipóteses de afastamentos, licenças e penalidades de suspensão, previstas na Lei nº 8.112, de 11 de dezembro de 1990, condição na qual a conta de acesso deve ser bloqueada a pedido da Coordenação-Geral de Pessoal, via Sistema GLPI;

V – imediatamente quando do desligamento, afastamento ou licença de usuário funcionário de empresa prestadora de serviço, para que seja efetuado o bloqueio momentâneo ou revogação definitiva da conta de acesso à rede e aos recursos de TIC, a pedido do Gestor do Contrato, via Sistema GLPI; e

VI - após decorridos 30 (trinta) dias consecutivos quando do desligamento, afastamento ou licença de usuário servidor de órgão ou entidade que utiliza a infraestrutura de rede e serviços de TIC da Sudam, para que seja efetuado o bloqueio momentâneo ou a revogação definitiva da conta de acesso à rede e aos recursos de TIC, a pedido do Gabinete da Sudam, via Sistema GLPI, após ser comunicado formalmente pela órgão ou entidade.

Art. 26. O desbloqueio da conta de acesso à rede local será realizado apenas após solicitação formal do superior imediato do usuário à Divisão de Infraestrutura Tecnológica, através do Sistema GLPI.

Parágrafo único. No caso de usuários de órgãos ou entidades que utilizam a infraestrutura de rede e serviços de TIC da Sudam, a solicitação de desbloqueio de conta de acesso deverá ser formalizada através do Gabinete da Sudam.

Art. 27. A conta de acesso não utilizada há mais de 180 (cento e oitenta) dias poderá ser cancelada.

Art. 28. A Coordenação-Geral de Tecnologia da Informação e Comunicações deve configurar o bloqueio automático de sessão nos ativos de informação após um período de inatividade preestabelecido, que poderá ser específico para cada tipo de ativo.

Art. 29. A Coordenação-Geral de Tecnologia da Informação e Comunicações deve, sempre que possível, ao invés da exclusão definitiva, priorizar a revogação/desativação de contas de acesso com o objetivo de manter dados e logs para possíveis auditorias.

Seção IV

Da Conta de Acesso Biométrico

Art. 30. A conta de acesso biométrico, quando implementada, deve ser vinculada a uma conta de acesso lógico e ambas devem ser utilizadas para se obter um acesso, a fim de atender aos conceitos da autenticação de multifatores.

Parágrafo único. A Sudam deverá tratar seus respectivos dados biométricos como dados sigilosos, utilizando-se, preferencialmente, de criptografia, na forma da legislação vigente.

Seção V

Dos Administradores

Art. 31. A utilização de conta de acesso com perfil de administrador é permitida somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

§ 1º Somente os técnicos da Coordenação-Geral de Tecnologia da Informação e Comunicações, devidamente identificados e habilitados, terão senha com privilégio de administrador nos equipamentos locais, na rede, nos sistemas informatizados e serviços de TIC da Sudam.

§ 2º Na necessidade de utilização de conta de acesso com privilégio de administrador do equipamento local, o usuário deverá encaminhar solicitação para a Divisão de Infraestrutura Tecnológica, para avaliação e providências decorrentes.

§ 3º Se concedida a permissão ao usuário como administrador local na estação de trabalho, esse será responsável por manter a integridade da máquina, não podendo instalar, desinstalar ou remover qualquer programa sem autorização formal da Coordenação-Geral de Tecnologia da Informação e Comunicações.

§ 4º A conta de acesso com privilégio de administrador nos equipamentos locais será fornecida em caráter provisório, podendo ser renovada por solicitação formal do titular da unidade requisitante.

§ 5º Salvo para atividades específicas da Coordenação-Geral de Tecnologia da Informação e Comunicações, não será concedida, para um mesmo usuário, identificação (**login**) com privilégio de administrador para mais de uma estação de trabalho, ou para acesso a servidores de rede e a dispositivos de rede.

§ 6º Excepcionalmente, poderão ser concedidas contas de acesso à rede local e aos recursos de Tecnologia da Informação da Sudam para visitantes, em caráter temporário, após apreciação da Coordenação-Geral de Tecnologia da Informação e Comunicações por meio da Divisão de Infraestrutura Tecnológica.

§ 7º A Divisão de Infraestrutura Tecnológica deve preferencialmente implementar a autenticação de multifatores (MFA) para todas as contas de administrador.

§ 8º A Divisão de Infraestrutura Tecnológica deve, sempre que possível, restringir os privilégios de administrador apenas a contas de administrador local nos ativos de informação.

CAPÍTULO VI

DOS ACESSOS

Seção I

Do Acesso à Rede Local

Art. 32. O acesso à rede local da Sudam e aos recursos tecnológicos disponíveis poderá se dar através da infraestrutura de rede cabeada ou de rede sem fio.

Art. 33. A utilização da rede local da Sudam deve se restringir aos recursos tecnológicos necessários ao cumprimento das atividades e atribuições do usuário.

Art. 34. A rede local da Sudam é monitorada por ferramentas específicas sem, contudo, infringir o princípio da confidencialidade das informações, visando ao provimento de solução para análise de performance na rede ou outros problemas associados aos ativos de TIC conectados à rede e prejudiciais ao uso dos recursos pela Sudam.

Art. 35. Apenas poderão ser conectados à rede local da Sudam microcomputadores, notebooks e outros dispositivos móveis de propriedade da autarquia, previamente configurados e autorizados pela Coordenação-Geral de Tecnologia da Informação e Comunicações.

§ 1º Exceções ao disposto no caput devem ser comunicadas à Diretoria de Administração, justificando a necessidade e o prazo de utilização.

§ 2º As exceções autorizadas deverão, obrigatoriamente, adotar os padrões definidos pela Política de Segurança da Informação e Comunicações – POSIC/Sudam e suas normas complementares, sendo o proprietário do equipamento responsável pelo licenciamento dos produtos nele instalados, uma vez que a Sudam não fornecerá licenças para o funcionamento de dispositivos particulares.

Art. 36. Notebooks e outros dispositivos móveis particulares poderão acessar a rede sem fio específica para esse fim, comumente chamada de "rede visitante".

Parágrafo único. O usuário, antes de acessar a rede visitante, deverá se identificar e concordar com os termos de uso da rede sem fio.

Art. 37. A Divisão de Infraestrutura Tecnológica poderá desconectar das redes cabeada e sem fio qualquer dispositivo que constitua ameaça à segurança da informação.

Art. 38. Os computadores com acesso à rede local deverão ser desligados ou bloqueados na ausência do usuário.

Seção II

Do Acesso à Intranet e à Internet

Art. 39. Qualquer usuário cadastrado na rede local da Sudam tem direito ao acesso à internet, disponibilizado para uso dentro das suas atribuições, passível de auditoria.

Art. 40. O perfil de acesso dos usuários da Sudam à internet é padronizado.

Parágrafo único. Em caso de necessidade de acesso a sítios e/ou serviços não contemplados pelo perfil padrão, o gestor da unidade pode solicitar a alteração para análise da Coordenação-Geral de Tecnologia da Informação e Comunicações, via Sistema GLPI, contendo justificativa e o prazo pretendido.

Art. 41. Os acessos aos portais da internet e aos demais serviços disponíveis na intranet da Sudam serão efetuados, preferencialmente, por meio da rede local e deverão ser identificados por usuário.

Art. 42. Todas as operações de acesso à internet realizadas no âmbito da Sudam deverão ser feitas de forma autenticada (conta de acesso à rede local), para registro e armazenamento em sistemas de log, para fins de auditoria.

Parágrafo único. A Sudam se reserva ao direito de manter registro de sítios/páginas visitadas, registro de acesso a aplicações de internet, bem como o registro de conexão, pelo tempo que for necessário, por qualquer usuário interno que faça uso da internet disponibilizada no âmbito da autarquia, ou por qualquer usuário externo que acesse o sítio institucional e/ou os sistemas de informações disponibilizados pelo órgão na internet.

Art. 43. Os acessos aos sítios e serviços disponíveis na internet serão controlados por filtros de conteúdo e reguladores de tráfego implementados nos dispositivos de segurança da rede local da Sudam, cuja operacionalização é de responsabilidade da Divisão de Infraestrutura Tecnológica.

§ 1º Os titulares das unidades organizacionais da Sudam devem fiscalizar o bom uso dos acessos à internet e solicitar ajustes e restrições, em caso de má utilização.

§ 2º Mediante solicitação do titular da unidade organizacional, a Divisão de Infraestrutura Tecnológica poderá fornecer relatórios mensais dos acessos para permitir o devido controle.

Art. 44. É vedado burlar ou tentar burlar os filtros de conteúdo ou restrições de acesso à internet, sob pena de responsabilização dos envolvidos, que estarão sujeitos às sanções administrativas e penais cabíveis.

Art. 45. É vedado o acesso a sítios que tratem de pornografia, pedofilia, erotismo e correlatos; de racismo; de ferramentas para invasão e evasão de sistemas; de compartilhamento de arquivos; e de apologia e incitação a crimes.

Parágrafo único. A Coordenação-Geral de Tecnologia da Informação e Comunicações verificará regularmente o acesso à internet sem, contudo, infringir o princípio da confidencialidade das informações, com objetivo de detectar ameaças à segurança ou o seu uso indevido, podendo utilizar softwares específicos com funcionalidades de bloqueio manual, automático e proativo de domínios/sítios.

Art. 46. A Divisão de Infraestrutura Tecnológica poderá, eventualmente e quando necessário, fazer ajustes temporários no controle de banda para viabilizar eventos específicos como videoconferências e acesso a visitantes.

Art. 47. A utilização do acesso à internet disponibilizado pela Sudam deverá estar prioritariamente relacionada ao desempenho das funções do usuário.

Parágrafo único. O uso pessoal da internet, em caráter eventual, é permitido, desde que não consuma recursos significativos de tempo ou interfira na produtividade pessoal.

Seção III

Do Acesso aos Sistemas de Informação

Art. 48. Sistemas de Informação são os programas e aplicativos desenvolvidos ou modificados pela Sudam, que detém todos os seus direitos, de acordo com o art. 4º da Lei nº 9.609, de 19 de fevereiro de 1998, vedada a sua cópia e distribuição, salvo determinação da Superintendência.

Art. 49. O usuário dos sistemas de informação e seus dados deve ter pleno conhecimento da Lei Geral de Proteção a Dados – LGPD, tendo em vista sua obediência no trato com dados pessoais e dados sensíveis contidos nos bancos de dados armazenados na Sudam.

Art. 50. Perfis de acesso são um conjunto de permissões atribuídas a cada usuário para a devida utilização das diversas funcionalidades de um sistema de informação, de acordo com as suas atribuições.

§ 1º A concessão e exclusão de perfil de acesso de usuário aos sistemas de informação da Sudam devem ser solicitadas à Coordenação-Geral de Tecnologia da Informação e Comunicações pelo gestor da respectiva unidade organizacional, através do Sistema GLPI, contendo as informações necessárias.

§ 2º A permissão de acesso do usuário aos sistemas de informação da Sudam é válida pelo tempo determinado pelo solicitante ou pelo tempo de permanência na Unidade Organizacional.

§ 3º Compete ao solicitante definir o perfil adequado do usuário, de forma justificada.

Art. 51. Poderão possuir perfis de acesso aos sistemas de informação da Sudam os usuários discriminados no inciso XXII do art. 2º, no todo ou em parte, de acordo com as suas funções e atribuições, devidamente cadastrados conforme art. 15.

Art. 52. O acesso aos sistemas de informação institucionais é uma concessão da Sudam e será obrigatoriamente desabilitado quando do desligamento do usuário.

§ 1º Nos casos de afastamento temporário do usuário, o perfil de acesso aos sistemas de informação poderá permanecer ativo mediante solicitação formal do gestor da unidade organizacional à Divisão de Infraestrutura Tecnológica, através do Sistema GLPI.

§ 2º Em função da integração entre conta de acesso à rede e perfil de acesso sistêmico, o cancelamento, bloqueio, suspensão e desbloqueio do perfil de acesso aos sistemas de informação da Sudam seguem as condições descritas na Seção III do Capítulo V desta Norma Complementar.

Art. 53. Todas as solicitações de criação e alteração de perfis são armazenadas para a necessidade de auditorias futuras.

Seção IV

Da Utilização do Correio Eletrônico Corporativo

Art. 54. A Sudam disponibilizará uma conta de correio eletrônico corporativo individual para os servidores ocupantes de cargo efetivo ou cargo em comissão e para ocupantes de emprego público em exercício no órgão.

§ 1º Uma conta de correio eletrônico corporativo única também deverá ser disponibilizada para cada unidade organizacional até o nível de Coordenação-Geral.

§ 2º Em caso de necessidade de disponibilização de conta de correio eletrônico corporativo para unidades organizacionais abaixo do nível de Coordenação-Geral ou para Comissões, uma solicitação formal deverá ser encaminhada à Diretoria de Administração, de forma justificada.

Art. 55. O correio eletrônico corporativo é o recurso de comunicação a ser utilizado de modo compatível com o exercício da função, sem comprometer a imagem da Sudam e nem o tráfego de dados na rede local da instituição.

§ 1º Todas as mensagens eletrônicas enviadas e recebidas no domínio da Sudam (sudam.gov.br) terão registrados os dados de: data e hora do envio ou recebimento, remetente e destinatário.

§ 2º A Divisão de Infraestrutura Tecnológica deverá implementar mecanismos que evitem o envio e a recepção de mensagens que possam comprometer a segurança do serviço de correio eletrônico.

§ 3º A Divisão de Infraestrutura Tecnológica poderá estabelecer cotas para limitar o espaço de armazenamento das caixas postais, por Unidade Organizacional e por usuário.

§ 4º A Divisão de Infraestrutura Tecnológica não acessará mensagens individuais de caixas de e-mail, salvo para atender aos seguintes objetivos:

I - verificar a obtenção, retenção, uso e divulgação de informações por meio ou com fins ilícitos, ou em desacordo com a POSIC/Sudam e suas normas complementares, mediante autorização do Comitê de Governança Digital da Sudam;

II - recuperar conteúdo de interesse da Sudam, no caso de afastamentos legais do usuário e de seu substituto, mediante autorização do Comitê de Governança Digital da Sudam;

III - atender à demanda formulada no âmbito de processo administrativo disciplinar, mediante autorização do Comitê de Governança Digital da Sudam;

IV - atender à determinação judicial; e

V - realizar a recuperação de mensagens do **backup**, a pedido do próprio usuário.

§ 5º O envio de mensagens a componentes da lista de endereços e grupos de e-mails da Sudam restringir-se-á a assuntos de interesse geral da instituição.

Art. 56. A utilização do correio eletrônico corporativo é uma concessão da Sudam e será obrigatoriamente cancelada quando do desligamento do usuário, após realização de procedimento de **backup** da caixa postal.

§ 1º Nos casos de afastamento temporário do usuário, o acesso à sua caixa postal poderá permanecer ativo mediante solicitação formal do gestor da unidade organizacional à Divisão de Infraestrutura Tecnológica, através do Sistema GLPI.

§ 3º Em função da integração entre conta de acesso à rede e a caixa postal do usuário, o cancelamento, bloqueio, suspensão e desbloqueio da conta de correio eletrônico corporativo seguem as condições descritas na Seção III do Capítulo V desta Norma Complementar.

Art. 57. São vedadas as seguintes ações relacionadas à utilização do correio eletrônico corporativo:

I - acesso ou tentativa de acesso não autorizados a caixas postais do domínio sudam.gov.br, salvo nos casos previstos no § 4º do art. 55 desta Norma Complementar;

II - envio ou armazenamento de mensagem de conteúdo incompatível com as atribuições do usuário, incluindo as que contém ofensas, comentários discriminatórios e/ou pornografia; e

III - adulteração de dados referentes à origem da mensagem nos campos de controle e cabeçalho.

Art. 58. A Divisão de Infraestrutura Tecnológica prestará suporte para a configuração e utilização da tecnologia adotada para o serviço de correio eletrônico corporativo.

Art. 59. O correio eletrônico particular deverá ser usado somente para interesses particulares do usuário, não podendo ser utilizado para o envio ou recebimento de informações da Sudam.

Parágrafo único. A Sudam não se responsabilizará em fornecer suporte técnico ao correio eletrônico particular, ficando a cargo do usuário as configurações e resolução de problemas.

Seção V

Da Utilização do Sistema de Arquivos

Art. 60. O sistema de arquivos compreende um conjunto de pastas armazenadas em servidor de arquivos e compartilhadas na rede local da Sudam, que podem ser compartilhadas entre todos os usuários ou restritas a usuários de determinada Unidade Organizacional ou de determinado projeto.

Art. 61. A Divisão de Infraestrutura Tecnológica realizará o **backup** dos arquivos armazenados no servidor de arquivos, conforme discriminado na Política de Backup da Sudam.

Parágrafo único. O **backup** de arquivos de pastas de usuário armazenadas nas estações de trabalho é de responsabilidade do usuário.

Art. 62. A Divisão de Infraestrutura Tecnológica poderá limitar o tipo de extensão dos arquivos a serem armazenados nas pastas das Unidades Organizacionais.

Art. 63. A Divisão de Infraestrutura Tecnológica não acessará os arquivos armazenados nas pastas das Unidades Organizacionais e dos usuários, salvo nas seguintes situações:

I - para verificar a obtenção, retenção, uso e divulgação de informações por meio ou com fins ilícitos, ou em desacordo com a POSIC/Sudam e suas normas complementares, mediante autorização do CGD;

II - para recuperar conteúdo de interesse da Sudam, no caso de afastamentos legais do usuário e de seu substituto, mediante autorização do CGD;

III - para atender à demanda formulada no âmbito de processo administrativo disciplinar, mediante autorização do CGD;

IV - para atender à solicitação judicial; e

V - para realizar a recuperação de arquivos do **backup**, a pedido do usuário.

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 64. Os incidentes que afetem a segurança das informações institucionais, assim como o descumprimento da POSIC/Sudam e das suas normas complementares, devem ser obrigatoriamente comunicados pelos usuários à Coordenação-Geral de Tecnologia da Informação e Comunicações, que em concomitância às ações de mitigação e solução encaminhará as informações à Equipe de Tratamento e Resposta a Incidentes Cibernéticos da Sudam.

Art. 65. Em caso de suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, a Coordenação-Geral de Tecnologia da Informação e Comunicações fará a investigação em conjunto com a Equipe de Tratamento e Resposta a Incidentes Cibernéticos da Sudam, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

§ 1º Nos casos em que o autor da quebra de segurança da informação for um usuário interno, a Coordenação-Geral de Tecnologia da Informação e Comunicações comunicará os resultados do incidente ao respectivo superior imediato para adoção de medidas cabíveis.

§ 2º As ações que violem esta norma complementar, a POSIC/Sudam ou que quebrem os controles de segurança da informação serão passíveis de sansões civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente.

§ 3º Deverá ser instaurado processo administrativo disciplinar específico para apurar as ações que constituem em quebra das diretrizes impostas por esta norma e pela POSIC/Sudam.

Art. 66. Os casos omissos serão dirimidos pelo Comitê de Segurança da Informação e Comunicações da Sudam.