RESOLUÇÃO LEGISLATIVA Nº 006/2015

Dispõe sobre a política de Segurança da Informação no âmbito dos Sistemas de Comunicação da Assembleia Legislativa do Estado de Roraima e dá outras providências.

A MESA DIRETORA DA ASSEMBLEIA LEGISLATIVA DO ESTADO DE RORAIMA, no uso de suas atribuições legais, faz saber que o Plenário aprovou e ela promulga a seguinte Resolução:

Art. 1º De acordo com os princípios da moralidade, impessoalidade, publicidade, eficácia e razoabilidade, esta Resolução dispõe sobre a Política de Segurança da Informação no âmbito dos Sistemas de Comunicação desta Casa Legislativa, objetivando educar o usuário e disciplinar a utilização das tecnologias disponibilizadas a serviço das atividades do Legislativo Estadual.

Art. 2º A Política de Segurança constante desta norma visa, primordialmente, proteger as informações constantes dos sistemas e software desenvolvidos ou adquiridos por esta Casa Legislativa.

Art. 3º O acesso dos sistemas é livre, porém disciplinado, de maneira que somente os responsáveis por determinadas tarefas ou setores podem ter acesso a qualquer momento.

Art. 4º Fica aprovado o Manual de Normas Gerais, constante da Política de Segurança da Informação, como parte integrante anexa ao presente instrumento normativo.

Art. 5º A Mesa Diretora editará normas complementares, se necessário, ao fiel cumprimento desta e aprimoramento dos sistemas.

Art. 6º Esta Resolução Legislativa entra em vigor na data de sua publicação.

Palácio Antônio Martins, 23 de junho de 2015.

Deputado **JALSER RENIER**
Presidente

Deputado **NALDO DA LOTERIA**
1º Secretário

Deputado **MARCELO CABRAL**
2º Secretário

RESOLUÇÃO LEGISLATIVA Nº 006/15

ANEXO I – MANUAL DE NORMAS GERAIS

DIRETORIA DE MODERNIZAÇÃO INSTITUCIONAL E TECNOLÓGICA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

NORMAS GERAIS DE UTILIZAÇÃO DA REDE, E-MAIL CORPORATIVO E ACESSO À INTERNET

SUMÁRIO

1 APRESENTAÇÃO

Este documento trata especificamente das normas elaboradas pela Diretoria de Modernização Institucional e Tecnológica – **DMIT**, tendo por finalidade estabelecer as diretrizes para a segurança do manuseio, tratamento, controle e para a proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos por qualquer meio pelos sistemas de informação a serem, obrigatoriamente, observados na definição de regras operacionais e procedimentos no âmbito da **Assembleia Legislativa do Estado de Roraima – ALERR**;

Tendo em vista:

- Segurança da Informação;
- Preservação do Patrimônio;
- Eficiência e Eficácia no Suporte;
- Controle na Utilização da Internet, Rede e E-Mail;
- Qualidade na Prestação do Serviço Público.

Esta diretoria apresenta normas para utilização dos recursos acima referidos, de forma a preservar o patrimônio e a informação, no que se refere aos setores computacionais e de comunicação, e a reputação da Assembleia Legislativa do Estado de Roraima – **ALERR**.

2 OBJETIVOS

2.1 OBJETIVO GERAL

Normatizar as atividades referentes a serviços oferecidos, como acesso à Internet, Intranet, e-mail e rede de dados da Assembleia Legislativa do Estado de Roraima, tendo como finalidade maior o aumento na segurança das informações desta instituição, estabelecendo procedimentos para viabilizar o serviço eficiente e eficaz.

2.2 OBJETIVOS ESPECÍFICOS

Esta norma tem como objetivo específico integrar-se à **Política de Segurança da Informação da ALERR**, em seu momento inicial de implantação, podendo vir a ser substituída ou conviver junto às demais normas de segurança futuramente elaboradas, visando, de forma geral, a proteção do ambiente tecnológico no intuito de prevenir e responder a possíveis incidentes de segurança. Sua abrangência estende-se a todos os usuários dos recursos computacionais da **Assembleia Legislativa do Estado de Roraima**, incluindo empregados, servidores, terceirizados, estagiários, técnicos dos núcleos setoriais de informática e os que, de alguma forma, se utilizem dos recursos de rede interna da **ALERR**.

Ressalta-se que, primordialmente, todos os que necessitem ter acesso aos recursos de rede da ALERR deverão, como condição, assinar "**Termo de Responsabilidade**", comprometendo-se à estrita observância e obediência às normas para o acesso aos recursos computacionais, cujo descumprimento incorrerá nas penalidades cabíveis, de acordo com a infração cometida e penalidades previstas em legislação competente.

Esta política encontra-se dividida nos seguintes tópicos:

I. Utilização dos recursos de Rede e Dispositivos;
II. Utilização do E-mail corporativo;
III. Utilização do acesso à Internet;

Também é de interesse desta norma:

a) Informar ao usuário quais os procedimentos para a correta utilização dos serviços de intranet e internet oferecidos pela ALERR, tais como correio eletrônico, acesso a sites etc;

b) Informar ao usuário a correta utilização da sua conta de acesso aos computadores e e-mail desta Casa;

c) Definir os tipos de perfis de acesso a conteúdo na Internet;

d) Informar as permissões

3 DAS CONTAS DE USUÁRIO

Para facilitar a identificação, tanto de usuários como dos recursos de rede computacionais interligados, os mesmos deverão seguir os padrões abaixo especificados.

3.1 POLÍTICA DE USUÁRIOS E GRUPOS ADMINISTRATIVOS

O uso de atribuições unificadas de usuário (LOGIN, E-MAIL, INTRANET E INTERNET) servem como agente facilitador na manutenção, dado a demanda e a necessidade do cadastramento de usuário ou grupo de trabalho. A inclusão da permissão de uso de tais recursos se dão através de requerimento e termo declaratório de ciência, com prévia informação de restrição e permissões. Este termo pode ser solicitado junto à DMIT que fornecerá instruções ademais sobre o preenchimento e permissões. Ao assiná-lo, o usuário torna formalmente comprovável sua ciência e alega concordar com o descrito que segue em anexo neste documento (ANEXO II).

As permissões espontâneas e/ou diferenciadas, permanentes ou não, deverão ser solicitadas por chefia imediata ou por superior hierárquico, conforme cronograma disposto na RESOLUÇÃO LEGISLATIVA Nº 009/11.

3.2 USUÁRIO

Os usuários que possuírem direitos de acesso à rede local (LAN) Intranet da ALERR e ainda ao serviço de correio eletrônico (E-mail) deverão obedecer ao seguinte padrão de nomes de usuário/login:

Modelo: **primeiro_nome.inicial_sobrenome+inicial_sobrenome**
Exemplo:
Nome do usuário: **José Maria Silva**
Login: **jose.ms**
Para todos os usuários da área administrativa da ALERR, o e-mail do usuário será o seu login de rede seguido do domínio **"@al.rr.leg.br".**
Exemplo:

Login de usuário na rede local: **jose.ms**
Endereço de e-mail: **jose.ms@al.rr.leg.br**

3.3 PERFIL PADRÃO DE ACESSO À INTERNET

Os sites na Internet estarão agrupados por categorias.

O perfil de acesso padrão à Internet obedecerá as seguintes regras, organizadas por categoria:

Sites com conteúdo de pesquisa e acesso a informações que estarão disponíveis:

- Fontes de Notícias
- Provedores de Pesquisa
- Webmail
- Finanças e Investimentos
- Bancos
- Portais Institucionais
- Portais Governamentais

Sites que estarão indisponíveis (Salvo uso designado por atribuições funcionais administrativas):

- Bate-papo
- Música e MP3
- Violência
- Armazenamento de arquivos
- Rádio e TV
- Blogs/Fotolog
- Redes sociais
- Downloads de software
- Navegação anônima

As demais categorias não contidas acima serão definidas como indisponíveis, como:

- Erotismo e Nudez
- Hackers
- Jogos de Azar
- Jogos eletrônicos
- Namoros
- Sexo
- Ganhe navegando
- Relacionamentos
- Procura de Emprego

4 NORMAS GERAIS DE UTILIZAÇÃO DA REDE, E-MAIL E ACESSO À INTERNET

Abaixo estão descritas as normas relacionadas que trazem como premissa básica o conceito de que tudo o que não for permitido e/ou liberado é considerado violação à **Política de Segurança da Informação.**

Salienta-se que, em virtude de ser a segurança da informação um processo contínuo e de estar a DMIT em pleno processo de elaboração e implantação de sua Política de Segurança da Informação, novas normas e possíveis alterações de versão estarão sendo implementadas, neste último caso, revogando-se, automaticamente, a norma anterior, devendo, portanto, todos os que fazem uso dos recursos computacionais da ALERR, manterem-se atualizados e obedientes às normas em vigor que estarão disponibilizadas em nossa Intranet (intranet.al.rr.gov.br/DMIT/politicas.html) para fins de conhecimento.

4.1 DA UTILIZAÇÃO DOS RECURSOS DE REDE E DISPOSITIVOS

Esse tópico visa definir as normas de utilização da rede e de dispositivos da ALERR.

A) Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta. Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário, ou colocar à prova a segurança de outras redes;

B) Não é permitida a conexão de dispositivos não autorizados na rede local, principalmente equipamentos de rede sem fio como roteadores, modens, hubs, entre qualquer outra solução que estabeleça conexão simultânea com a rede local e outras redes. Em casos justificados para o uso destes equipamentos, a **DMIT** deve prover segmento de rede independente, através de VLAN (Ambiente virtualizado de rede) para este fim, de forma a permitir o compartilhamento de sua infraestrutura de TI, sem o comprometimento do desempenho e da segurança da rede local;

C) Profissionais no exercício de suas funções, que necessitem de comunicação externa, deverão solicitar à DMIT a providência de seguimento de rede independente;

D) A inclusão de novos equipamentos na rede interna deverá ser executada pela Unidade destinada a estes fins. O privilégio de administrador deverá ficar sob a responsabilidade da Unidade que efetua tais instalações, restando ao usuário, ao qual se destina o equipamento, utilizá-lo mediante credenciais de “usuário comum”. Ressalva-se o caso de usuários da área técnica, devidamente autorizados, que por força de suas funções e conhecimento técnico assumam as respectivas responsabilidades de efetuar suas próprias instalações. No mais, ressalta-se a necessidade de conformidade com as demais políticas vigentes. Posteriormente, a DMIT deverá ser comunicada para futuras auditorias. No caso de novos servidores, estes equipamentos deverão ser configurados e administrados pela DMIT;

E) Caso seja necessária a inclusão de máquinas previamente em uso em outras redes e transferidas para o ambiente da ALERR, deverá ser feita análise prévia de conformidade das instalações com as políticas vigentes, de forma a adequá-las aos padrões exigidos, evitando-se riscos de comprometimento da performance e segurança da rede;

F) Não são permitidas tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques do tipo negação de serviço (DoS), provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de "quebrar" (invadir) um servidor;

G) Não é permitido o uso de qualquer tipo de programa não relacionado às funções e atividades pertinentes à ALERR;

H) Instalações e/ou remoções de softwares deverão ser efetuadas pela Unidade destinada a estes fins;

I) Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas acessados, evitando, desta maneira, o acesso por pessoas não autorizadas, bem como efetuar o *logout/logoff* da rede ou bloqueio da estação de trabalho através de senha;

J) É de responsabilidade do servidor o armazenamento dos arquivos importantes para o desempenho das funções na unidade de rede. Caso necessário, o usuário poderá solicitar acompanhamento de um técnico para confirmação da cópia de segurança;

K) É vedada a abertura de computadores para qualquer tipo de reparo, uma vez que, qualquer reparo necessário deverá ser feito pelo departamento técnico responsável;

L) Não será permitida a alteração das configurações de rede (principalmente endereço IP) e da BIOS das máquinas, bem como modificações que possam trazer algum problema futuro;

M) É de responsabilidade do usuário manter o sigilo das suas senhas de acesso à rede e aos sistemas;

N) No que se refere a equipamentos que integrem a rede local da ALERR, a DMIT se reserva ao direito de realizar monitoramentos e relatórios;

4.2 UTILIZAÇÃO DO E-MAIL CORPORATIVO

Esse tópico visa definir as normas de utilização do e-mail corporativo.

a) O e-mail corporativo deve ser de uso restrito para as atividades relacionadas ao desempenho das funções do funcionário, sendo considerado o meio formal de comunicação eletrônica na ALERR;

b) É proibido o assédio ou perturbação de outrem, seja através de linguagem utilizada, frequência ou tamanho das mensagens;

c) É proibido o envio de grande quantidade de mensagens de e-mail ("*junk mail*" ou "*spam*") que, de acordo com a capacidade técnica da Rede, seja prejudicial ou gere reclamações de outros usuários. Isso inclui qualquer tipo de mala direta, como, por exemplo, publicidade, comercial ou não, anúncios e informativos, ou propaganda política. Ressalva-se, neste caso, que fica preservado o direito de envio de e-mail para todos os servidores por parte da ALERR, quando se fizer necessário;

d) É proibido reenviar ou, de qualquer forma, propagar mensagens em cadeia ou "correntes", independentemente da vontade do destinatário de receber tais mensagens;

e) Caso a ALERR julgue necessário haverá bloqueios:

- ✓ De e-mail com arquivos anexos que comprometa o uso de banda, perturbe o bom andamento dos trabalhos, ou ainda, exponha a rede a riscos de segurança. Arquivos com

código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) e outras extensões comumente utilizadas por vírus são automaticamente bloqueadas.

✓ De e-mail para destinatários ou domínios que comprometa o uso de banda, perturbe o bom andamento dos trabalhos ou ainda, exponha a rede e o ambiente destinatário a riscos de segurança.

4.3 – **UTILIZAÇÃO DO ACESSO À INTERNET**

Esse tópico visa definir as normas de utilização da Internet.

a) É proibido utilizar os recursos da ALERR para fazer o *download* ou distribuição de software ou dados não legalizados;

b) É proibida a divulgação de informações confidenciais da ALERR em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida;

c) Os usuários da área técnica, devidamente autorizados, somente poderão efetuar download de softwares necessários à execução de suas atribuições, devendo providenciar, quando for o caso, a regularização da licença e o registro desses, de forma a evitar possíveis penalidades à ALERR;

d) Caso esta Casa julgue necessário, haverá bloqueios de acesso a arquivos e sites não autorizados que comprometam o uso de banda da rede, o desempenho e produtividade das atividades do servidor, bem como que exponham a rede a riscos de segurança;

e) É proibida a utilização de meios para burlar as políticas de bloqueios automaticamente aplicadas no proxy da ALERR, como web-proxy e tunelamentos criptografados.

f) Haverá geração de relatórios dos sites acessados por usuário para verificação da adequação à política vigente;

g) Não será permitido o uso de comunicação instantânea como MSN, Skype e afins;

h) Recursos e relatórios serão enviados para as respectivas gerências, para as devidas providências;

i) Não será permitida a utilização de softwares *peer-to-peer* (P2P), tais como Emule, Kazaa, Morpheus e afins;

j) A utilização de serviços de redes sociais, além de *streaming* de áudio e/ou vídeo, será controlada quanto ao seu uso e excessos, ressalvando-se aqueles serviços pertinentes às atividades da ALERR.

5 PENALIDADES

As penalidades cabíveis, como os procedimentos de processo administrativo por omissão ou desrespeito, serão aplicadas conforme a **LEI COMPLEMENTAR Nº 53, DE 31 DE DEZEMBRO DE 2001 – RORAIMA**, que dispõe sobre o Regime Jurídico dos Servidores Públicos Civis do Estado de Roraima, e dá outras providências.

ANEXO I – LISTA DE DEFINIÇÕES

DEFINIÇÕES

Para os efeitos e aplicações desta norma são adotadas as seguintes definições técnicas:

1) **Acesso Remoto:** ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário;

2) **Auditoria:** verificação e avaliação dos sistemas e procedimentos internos, com o objetivo de reduzir fraudes, erros, práticas ineficientes ou ineficazes;

3) **Autenticação:** é o ato de confirmar que algo ou alguém é autêntico, ou seja, uma garantia de que qualquer alegação de ou sobre um objeto é verdadeira;

4) **Banco de Dados (ou Base de Dados):** é um sistema de armazenamento de dados, ou seja, um conjunto de registros que tem como objetivo organizar e guardar as informações.

5) **Bloqueio de acesso:** processo que tem por finalidade suspender temporariamente o acesso;

6) **Confidencialidade:** propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

7) **Controle de Acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

8) **Cópia de Segurança (Backup):** copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade. Essencial para dados importantes;

9) **Correio Eletrônico:** é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;

10) **Credenciais ou contas de acesso:** permissões concedidas por autoridade competente, após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física, como crachá, cartão e selo, ou lógica, como identificação de usuário e senha;

11) **Criptografia:** é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta ou senha");

12) **Dado:** representação de uma informação, instrução ou conceito, de modo que possa ser armazenado e processado por um computador;

13) **Diretriz**: descrição que orienta o que deve ser feito e como, para se alcançar os objetivos estabelecidos nas políticas;

14) **Download:** (Baixar) copiar arquivos de um servidor (site) na internet para um computador pessoal;

15) **FTP (File Transfer Protocol):** (Protocolo de Transferência de Arquivo) é um protocolo da Internet para transferência de arquivos;

16) **Hardware:** É a parte física do computador, conjunto de componentes eletrônicos, circuitos integrados e periféricos, como a máquina em si, placas, impressora, teclado e outros;

17) **HTTP (Hyper Text Transfer Protocol):** (Protocolo de Transferência de Hipertexto) é uma linguagem para troca de informação entre servidores e clientes da rede;

18) **HTTPS (HyperText Transfer Protocol Secure)**: (Protocolo de Transferência de Hipertexto Seguro) é uma linguagem para troca de informação entre servidores e clientes da rede, com recursos de criptografia, autenticação e integridade;

19) **Incidente de Segurança:** é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

20) **Informação:** dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

21) **Informação sigilosa:** informação submetida temporariamente à restrição de acesso público, em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

22) **Internet:** rede mundial de computadores;

23) **Internet Protocol:** (Protocolo de Internet) é um protocolo de comunicação usado entre duas ou mais máquinas em rede para encaminhamento dos dados;

24) **Intranet:** rede de computadores privada que faz uso dos mesmos protocolos da Internet. Pode ser entendida como rede interna de alguma instituição em que geralmente o acesso ao seu conteúdo é restrito;

25) **Log:** é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para reestabelecer o estado original de um sistema, ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais;

26) **Logon:** Procedimento de identificação e autenticação do usuário nos Recursos de Tecnologia da Informação. É pessoal e intransferível;

27) **On line:** (Estar disponível ao vivo) no contexto da Internet significa estar disponível para acesso imediato, em tempo real;

28) **Perfil de acesso:** conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

29) **Peer-to-peer (P2P):** (Ponto a ponto) permite conectar o computador de um usuário a outro, para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens, entre outros;

30) **Política de Segurança da Informação:** documento aprovado pela autoridade responsável, pelo órgão ou entidade da Administração Pública Estadual, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;

31) **Proxy:** é um serviço intermediário entre as estações de trabalho de uma rede e a Internet. O servidor de rede proxy serve para compartilhar a conexão com a Internet, melhorar o desempenho do acesso, bloquear acesso a determinadas páginas;

32) **Quebra de segurança:** ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

33) **Recursos Computacionais:** recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;

34) **Rede Corporativa:** conjunto de todas as redes locais sob a gestão da instituição;

35) **Roteador:** equipamento responsável pela troca de informações entre redes;

36) **Segurança da Informação e Comunicações:** ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

37) **Servidor de Rede:** recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas informáticos;

38) **Servidor:** pessoa legalmente investida em cargo público;

39) **Software:** são todos os programas existentes em um computador, como sistema operacional, aplicativos, entre outros;

40) **Site:** Conjunto de páginas virtuais dinâmicas ou estáticas, que tem como principal objetivo fazer a divulgação da instituição;

41) **Streaming:** transferência de dados (normalmente áudio e vídeo) em fluxo contínuo por meio da Internet;

42) **Switches:** Um switch de rede é um equipamento eletrônico de comutação que funciona como um nó central numa rede no formato estrela, armazenando, em memória, o endereço físico de todos os computadores conectados a ele, relacionando cada endereço físico a uma de suas portas e permitindo assim a interligação entre os dispositivos conectados;

43) **Termo de Responsabilidade:** termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

44) **Trilhas de Auditoria:** são rotinas específicas programadas nos sistemas para fornecerem informações de interesse da auditoria. São entendidas como o conjunto cronológico de registros (logs) que proporcionam evidências do funcionamento do sistema. Esses registros podem ser utilizados para reconstruir, rever/revisar e
examinar transações desde a entrada de dados até a saída dos resultados finais, bem como para avaliar/rastrear o uso do sistema, detectando e identificando usuários não autorizados;

45) **Usuário:** servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da APF, formalizada por meio da assinatura do Termo de Responsabilidade;

46) **VLAN:** (Virtual Local Area Network ou Virtual LAN) – (Rede Local Virtual) é um agrupamento lógico de estações, serviços e dispositivos de rede que não estão restritos a um segmento físico de uma rede local;

47) **VPN (Virtual Private Network):** (Rede Privada Virtual) é uma rede de dados privada que faz uso das infraestruturas públicas de telecomunicações, preservando a privacidade, logo é a extensão de uma rede privada que engloba conexões com redes compartilhadas ou públicas. Com uma VPN pode-se enviar dados entre dois computadores através de uma rede compartilhada ou pública, de uma maneira que emula uma conexão ponto a ponto privada;

48) **Wireless (rede sem fio):** rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

ANEXO II – TERMO DE RESPONSABILIDADE

TERMO DE RESPONSABILIDADE

Política de uso da rede corporativa, computadores, internet e utilização de e-mails corporativos.

Eu,_____
____
Setor:_____Função:_____CPF:_____
-____ Usuário:_____ Matrícula:
_____Telefone:_____

Declaro haver solicitado acesso à rede corporativa, computadores, Internet e/ou utilização de e-mail coorporativo, comprometendo-me a:

a) Acessar a rede corporativa, computadores, Internet e/ou utilização de e-mail coorporativo, somente com autorização (usuário/senha), por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, normas e disposições contidas em Políticas de Segurança da Informação da Assembleia Legislativa do Estado de Roraima, disponível no endereço intranet.al.rr.gov.br/DMIT/politicas.html;

b) Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial;

c) Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

d) Não me ausentar da estação de trabalho sem encerrar a sessão de uso do navegador (browser), sem bloquear estação de trabalho, bem como encerrar a seção do e-mail corporativo, garantindo assim a impossibilidade de acesso indevido por terceiros;

e) Não revelar minha senha de acesso à rede corporativa, computadores, Internet e/ou de minha caixa postal (e-mail) coorporativo a ninguém e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento;

f) Alterar minha senha, sempre que obrigatório ou que tenha suspeita de descoberta por terceiros, não usando combinações simples que possam ser facilmente descobertas;

g) Respeitar as normas de segurança e restrições de sistema impostas pelos sistemas de segurança implantados na ALERR;
h) Responder pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenha acesso.

Declaro, ainda, estar plenamente esclarecido e consciente que:
1. Não é permitida a navegação aos sites pertencentes às categorias abaixo:

- ✓ Pornográfico e de caráter sexual;
- ✓ Compartilhamento de arquivos (ex.: Atube, peer to peer, Bit Torrent, Emule, 4shared, etc.);
- ✓ Pornografia infantil (pedofilia);
- ✓ Apologia ao terrorismo;
- ✓ Apologia às drogas;
- ✓ Crackers;
- ✓ Redes Sociais (Orkut, Facebook, Meebo, Whatsapp, Youtube, Instagram, etc.);
- ✓ Violência e agressividade (racismo, preconceito, etc.);
- ✓ Violação de direito autoral (pirataria, etc.);
- ✓ Áudio e vídeo, salvo com conteúdo relacionado diretamente a atividades administrativas ou profissionais;
- ✓ Instant Messengers, Chats e Videoconferência;
- ✓ Conteúdo impróprio, ofensivo, ilegal, discriminatório e similares.

2. Não é permitida a troca de arquivos de vídeo ou música, bem como de quaisquer informações que estejam incluídas nas categorias acima;
3. É proibida a transferência de qualquer tipo de programa, inclusive jogos e similares, para a rede interna da ALERR, à exceção de servidores da DMIT, com autorização específica para tal;
4. É proibido downloads de arquivos executáveis e de mídias, tais como: .exe, .mp3, .wav, .bat, .com, .sys, .scr, .ppt, .mpeg, .avi, .rmvb, .dll etc. Salvo os estritamente relacionados aos serviços inerentes à função do servidor

5. Não é permitido o acesso a programas de TV, Rádio e Entretenimento na internet, ou qualquer conteúdo sob demanda (streaming, buffer, etc.) salvo necessidade específica no exercício da função.
6. É proibido o uso de jogos, inclusive os de execução em browsers na internet (online);
7. O uso de e-mail corporativo não garante direito sobre este, nem confere autoridade para liberar acesso a outras pessoas, pois se constitui de informações pertencentes à ALERR;
8. Qualquer problema referente ao uso dos computadores da Rede de Computadores da ALERR, assim como ao uso da sua conta de e-mail corporativo da ALERR deverá imediatamente ser relatado à DMIT;
9. O usuário assumirá a responsabilidade por dano causado por algum procedimento de iniciativa própria de tentativa de modificação da configuração, física ou lógica, do computador e/ou rede sem a autorização expressa da DMIT;
10. O usuário assumirá a responsabilidade pelo dano que possa causar caso não venha a cumprir o disposto neste termo de responsabilidade.

Declaro, nesta data, ter ciência e estar de acordo com os procedimentos acima descritos, comprometendo-me a respeitá-los e cumpri-los plena e integralmente.

_____, _____ de _____ de _____.

_____ _____ _____

Assinatura do Servidor Chefia Imediata Responsável pelo Cadastro