PLURAL
INDÚSTRIA GRÁFICA

Política de Segurança da Informação

Índice

1. Objetivo

Esta Política define as Diretrizes da Segurança da Informação, visando preservar a integridade, confidencialidade e disponibilidade das informações da PLURAL.

Confidencialidade: garantia de que a informação é acessível somente a pessoas autorizadas;

Integridade: salvaguarda da exatidão e totalidade da informação e dos métodos de processamento;

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Descrição de uma conduta adequada e segura para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados, sejam acidentais ou intencionais.

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios da organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como resultado deste aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades.

Esta Política é aplicável a todas as informações sob a gestão da PLURAL, que podem existir de muitas maneiras: escrita em papel, armazenada e transmitida por correio ou através de meios eletrônicos, exibida em filmes ou falada em conversas formais ou informais. Seja qual for à forma apresentada ou o meio através do qual a informação seja apresentada ou compartilhada, ela deverá estar sempre protegida adequadamente, de acordo com controles definidos nesta política.

Esta política deve ser conhecida e seguida por todos que utilizam os recursos de processamento da informação de propriedade ou controlados pela PLURAL, sendo de responsabilidade de cada um o seu cumprimento.

As informações de propriedade ou controladas pela PLURAL devem ser utilizadas apenas para uso próprio de propósitos definidos. Os usuários não podem, em qualquer tempo ou sob qualquer propósito, apropriar-se dessas informações em benefício próprio.

2. Diretrizes

O cumprimento dessa política de segurança da informação é compromisso de todos da PLURAL que devem obedecer às seguintes diretrizes:

- Proteger as informações contra acesso, modificação destruição ou divulgação não autorizada;

- Assegurar que os recursos colocados à sua disposição sejam utilizados apenas para as finalidades operacionais da PLURAL;

- Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos em conformidade com esta política vigente da PLURAL;

- Garantir a continuidade do processamento das informações críticas aos negócios;

- Atender às normas internas que regulamentam as atividades da PLURAL e o seu mercado de atuação;

- Comunicar imediatamente a área de Tecnologia da Informação, quando ocorrer qualquer tipo de dúvida ou incidente, podendo causar algum risco as suas atividades.

- Cada usuário terá acesso somente às informações necessárias para o desempenho de seu trabalho. Para que isso seja possível, toda informação terá um gestor que definirá a autorização de acessos.

- O usuário após a assinatura do Formulário de Solicitação de Acesso terá uma identificação única, pessoal e intransferível que ficará armazenada no sistema todas as vezes que as informações forem acessadas.

- A administração da segurança da informação é exercida pela área de Tecnologia que cuidará de todos os aspectos referentes à implementação e a manutenção dos projetos de segurança da informação.

Mas lembre-se: cuidar da segurança da informação da PLURAL é responsabilidade de todos.

O não cumprimento destas regras é considerado falta grave, sujeitando o infrator a uma ação disciplinar apropriada, podendo inclusive, motivar demissão por justa causa e ou rescisão contratual.

3. Área de Aplicação

A política de segurança da informação deve ser seguida e respeitada por todos os funcionários, terceiros e estagiários que prestam serviço em todas as unidades de negócio da PLURAL que serão designados como usuários dos recursos e equipamentos conectados à rede de computadores da empresa ou dos meios convencionais de processamento, comunicação e guarda de informações. Todos os funcionários e estagiário devem assinar o Termo de Autorização, Responsabilidade e Confidencialidade que receberão juntamente com essa política, disponibilizados pela área de Recursos Humanos.

4. Normas Gerais

A conduta adequada à garantia da segurança das informações é norteada por um conjunto de regras que devem ser observadas por todos aqueles que têm acesso às informações da PLURAL.

A Tecnologia da Informação tem um papel fundamental na garantia da segurança da informação e por isso valida e homologa todos os programas e equipamentos utilizados na PLURAL. Não são permitidas cópias de softwares não licenciados, alterações de configuração das estações de trabalho ou quaisquer tipos de modificação tecnológica no ambiente informatizado sem prévia autorização.

Toda contratação de serviços de informática tais como: treinamento, desenvolvimento ou consultoria devem ser submetidos à apreciação prévia da área de Tecnologia, que deverá providenciar uma análise de custo/benefício para aprovação da diretoria da área.

Não é permitida a duplicação, empréstimo, transferência ou retirada de software para outros equipamentos, dentro ou fora da empresa.

Não é permitido o uso de jogos, utilização de programas de licença gratuita (freewares), de validade temporária (sharewares) ou fornecida como demonstração (demos). Só poderá ser realizada em casos de comprovada necessidade para o negócio, de forma legal e com autorização formal do gestor da área usuária, da área de Tecnologia, desde que não haja programas com a mesma finalidade já adquiridos ou homologados pela empresa.

Proteger os equipamentos sob custódia e desligá-los ao final do expediente é dever de todos os usuários.

5. Norma de Utilização da Internet

A Internet é uma rede mundial para recepção e transmissão de informações por meio de computadores interligados. O Acesso à internet deve seguir políticas e normas visando proteger a PLURAL contra ameaças interna e externas à segurança das informações que trafegam na Rede.

O serviço de Internet é disponibilizado exclusivamente para uso nas atividades profissionais. O acesso às páginas da Internet, por meio dos recursos disponibilizados pela PLURAL, caracteriza um instrumento de trabalho e, assim destina-se e limita-se à execução das atividades pertinentes à função. O usuário é responsável pelo uso e segurança de sua conta de acesso, devendo seu login e sua senha ser tratados de forma particular, confidencial e exclusiva, sendo de sua inteira responsabilidade toda e qualquer consequência da utilização indevida. A conexão à internet deve ser encerrada sempre que o usuário se ausentar de sua estação de trabalho ou ao término do uso da sessão.

O usuário deve conduzir adequadamente o uso da Internet, respeitando direitos autorais, regras de licenciamento de softwares, direitos de propriedade, privacidade e proteção de propriedade intelectual.

O acesso à Internet, por meio da rede corporativa, deve ser efetuado somente por equipamentos autorizados pela Área de Tecnologia. O acesso à Internet deverá ser efetuado em apenas uma estação de trabalho ou equipamento, por vez. O software de acesso à Internet deve ser homologado pela área de Tecnologia da PLURAL.

Todo acesso à internet é controlado e registrado em sistema. A PLURAL reserva-se no direito de examinar e de monitorar o acesso à Internet disponibilizada, em conformidade com os termos da Lei e de utilizar do conteúdo das trilhas de auditoria, sendo proibido:

a) Utilizar os recursos da PLURAL para fazer downloads (mp3, vídeos, programas diversos) de conteúdo que não seja para utilização no trabalho, distribuição de software de qualquer natureza e de dados não legalizados, bem como a distribuição destes;

b) Divulgar informações confidenciais da PLURAL ou de seus clientes em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as

penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei;

c) Acessar informações ilegais ou que possam ser consideradas ofensivas, intimidatórias, ameaçadoras ou similares, sendo que o usuário será responsabilizado pelos sites acessados e pelos arquivos copiados para a rede Interna da Instituição;

d) Acessar portais ou páginas com conteúdo de caráter obsceno, sexual, pornográfico, erótico, racista, constrangedor, difamatório, discriminatório ou preconceituoso (sexo, raça, etnia, religião, nacionalidade), ilegal, agressivo e abusivo ou de qualquer outra natureza, que atente contra a integridade moral e os bons costumes dos indivíduos ou de grupos da sociedade.

e) Copiar programas freeware, shareware ou que não tenham sido adquiridos pela formas legais e conformidade com as leis brasileiras e autorizado pela área de Tecnologia. A utilização de softwares não legalizados é considerada PIRATARIA e pode causar danos financeiros e de imagem para a PLURAL.

f) Utilizar softwares de peer-to-peer (P2P), tais como Kazaa, Morpheus, E-Mule e afins.

g) Utilizar serviços de streaming, tais como rádios on-line e afins, a não ser que o acesso seja inerente a trabalhos, pesquisas, negócios da PLURAL.

h) Utilizar softwares de comunicação instantânea, tais como ICQ, Microsoft Messenger (MSN), Yahoo Messenger ou outro software de comunicação e afins.

i) Acessar e propagar qualquer tipo de conteúdo malicioso, como vírus, worms, cavalos de tróia ou programas de controle de outros computadores, bem como spam.

j) Utilizar programas ou acessar páginas de bate-papo (chat).

k) Utilizar para jogos on-line, fóruns não profissionais, gincanas e concursos on-line.

l) Utilizar a rede para fins comerciais, ilegais ou imorais.

m) Utilizar para tentativa de ataque ou intrusão a outros computadores da rede interna ou externa.

n) Utilizar para cópia, distribuição ou armazenamento não autorizado de material ou software protegido por leis de direito autoral, por qualquer meio.

o) Utilizar Webmail particular (Terra, UOL, Gmail e etc.), a não ser que seja para fins de trabalho.

p) Acessar e/ou divulgar informações da PLURAL em Redes Sociais, tais como Facebook, Orkut, MySpace, Linkedin, Twitter e afins.

q) Disponibilizar a outro usuário sua conta de acesso, devendo seu login e sua senha ser tratados de forma particular, confidencial e exclusiva.

Caso a área de Tecnologia julgue necessário poderá efetuar bloqueios de acesso a arquivos, domínios e serviços de Internet que comprometam o uso de banda, a segurança da PLURAL ou o bom andamento dos trabalhos.

Haverá geração de relatórios para análise de segurança dos sites acessados pelos usuários e poderá haver restrição a determinados conteúdos / sites sem aviso prévio.

A inobservância do disposto nessa norma constitui falta grave, sujeitando os infratores à perda imediata do direito de acesso e na aplicação de medidas cabíveis.

6. Normas de Utilização do correio eletrônico

O Correio Eletrônico é uma ferramenta essencial ao dia-a-dia, permitindo agilidade na comunicação interna e externa. As mensagens e os documentos eletrônicos estão sujeitos às mesmas leis e normas aplicadas a documentos escritos. O uso não controlado ou apropriado desta ferramenta pode trazer ameaças reais, tais como:

- Criminal (devido uso inapropriado);
- Autoridades Regulatórias (devido uso inapropriado);
- Contaminação por vírus (recepção de softwares mal-intencionados);
- Quebra da confidencialidade (devido uso inapropriado);
- Danos a Imagem (devido uso inapropriado).

O objetivo desta política é assegurar que todos os funcionários, terceiros e estagiários da PLURAL conheçam suas responsabilidades sobre o uso do correio eletrônico e as sigam de forma adequada. Assim como qualquer recurso provido pelaPLURAL, o uso dos serviços do correio eletrônico deve ser dedicado às atividades de interesse da PLURAL regido por regras de conduta similares àquelas aplicáveis a outros recursos de informática. O uso adequado deve ser legal, ético, refletir honestidade e demonstrar moderação no consumo dos recursos compartilhados. O uso inapropriado dos serviços de correio eletrônico, em alguns casos, pode causar interrupção das atividades.

As mensagens enviadas através do e-mail corporativo não são consideradas como informação particular. Assim sendo a PLURAL reserva para si o direito de monitorar e inspecionar o uso do e-mail disponibilizado, em conformidade com os termos da Lei.

Por padrão será fornecido uma única caixa postal pessoal e intransferível.

Os usuários não devem violar direitos de propriedade de informação, mecanismos de segurança, e também não devem usar o correio eletrônico para intimidar, assediar ou causar transtornos.

Todas as mensagens ficam armazenadas em um servidor de e-mail que possui recursos limitados. Para que não ocorram problemas de indisponibilidade de caixas postais, o servidor bloqueia as mensagens

quando o usuário atinge sua cota de armazenamento. Com isso, o usuário deve periodicamente arquivar ou excluir as mensagens que não forem mais necessárias.

Poderá ser dado a um usuário o direito de acessar a caixa postal de outro usuário. Este procedimento pode ser realizado pelo usuário proprietário da caixa postal ou pela área de Tecnologia por meio de autorização por escrito do proprietário da caixa postal ou seu superior.

Não há qualquer procedimento específico (desativação ou exclusão) para ausências temporárias (férias ou licença). O usuário poderá configurar sua caixa postal para deixar de receber mensagens.

Não é permitida a utilização de Forward para encaminhamento de mensagens da PLURAL para endereços externos.

Só é permitida a criação de caixa postal para terceiros (fornecedores, prestadores de serviços, etc.), mediante autorização previa da gerência imediata, RH e área de Tecnologia.

Funcionários demitidos ou afastados terão a caixa postal bloqueada mediante solicitação formal do RH e excluídas após execução do backup mensal.

O conteúdo de qualquer mensagem de correio deve ser apropriado às atividades da PLURAL, sujeitando-se às mesmas restrições como qualquer outra correspondência.

É expressamente proibido aos usuários de correio eletrônico:

a) Transmitir material que seja considerado ofensivo, discriminatório, calunioso, fraudatório, danoso, ilegal ou que possa violar os padrões de ética e cortesia profissional.

b) Transmitir ou abrir material que contenha pornografia e conteúdo de assédio moral.

c) Transmitir piadas e conteúdo humorístico.

d) Transmitir arquivos executáveis como anexo e extensões que possibilitem a propagação de vírus: (.bat, .chm, .cmd, .dll, .exe, .hta, .inf, .js, .jse, .lnk, .pif, .scr, .vbs, .vxd). Esta lista está sujeita a alterações sem aviso prévio.

e) Transmitir SPAM (mensagens não solicitadas enviadas para vários destinatários com conteúdo não relacionado às atividades da PLURAL, como exemplo, divulgação comercial, autopromoção, etc.).

f) Participar de "pirâmides" e "correntes" (correspondência não relacionada aos negócios da empresa que seja replicada para muitos usuários).

g) Retransmitir e-mail, com arquivos anexos muito grandes, como, por exemplo, arquivos contendo fotos imagens, animações, filmes, multimídia, música etc., os quais podem interromper ou prejudicar o funcionamento dos servidores/equipamentos de outra pessoa ou causar problemas de performance no sistema.

h) Abrir arquivos anexos de origem duvidosa.

i) Colocar seus e-mails em chats e listas de discussão não relacionadas ao trabalho.

j) Colocar as suas opiniões pessoais como sendo aquelas da PLURAL.

k) Divulgar informações consideradas confidenciais ou proprietárias da PLURAL ou de seus clientes, enviar a terceiros informações relativas às atividades da PLURAL e de suas missões, exceto quando aprovadas formalmente pela diretoria, reenviar a terceiros comunicados recebidos quando expressamente não permitido.

l) Divulgar o endereço de e-mail de outros funcionários sem a anuência dos mesmos.

A PLURAL se reserva no direito de preservar seus equipamentos e recursos computacionais através da RECUSA do recebimento de mensagens cujos conteúdos não expressam o interesse da PLURAL, ou que possam colocar em risco o funcionamento dos sistemas.

Todas as mensagens são passíveis de monitoração e gravação quanto aos endereços de destino e origem (IP de origem, E-mail do remetente, IP de destino, E-mail do destinatário) e serão usados para estabelecer critérios de RECUSA.

Eventuais ações de leitura de E-mail pela administração do sistema podem ocorrer perante autorização do responsável pela caixa postal ou do gestor.

Para os casos de falha ou incompletude dos procedimentos previstos, bem como, no enfrentamento de situações inesperadas, a área de

Tecnologia poderá, a seu critério, suspender a conta de correio ou todo o serviço comunicando o fato à Diretoria.

As caixas postais do correio eletrônico, incluindo as informações contidas em seus arquivos, são propriedade da PLURAL, reservando-se a este, portanto, o direito de monitorar e gravar toda a atividade quando considerar necessário. O uso da caixa postal de correio eletrônico e dos demais recursos de informática indica o consentimento do usuário a essa monitoração e, quando necessário, à divulgação da PLURAL às autoridades competentes de quaisquer evidências que possam constituir crime, delito ou violação às atividades. A PLURAL poderá eventualmente realizar monitoração (auditoria) das caixas postais através da utilização de softwares específicos.

7. Normas de Controle de Acesso

Os profissionais e terceiros da PLURAL devem ter acesso físico e lógico liberado somente aos locais e recursos necessários ao desempenho de suas atividades e de conformidade aos interesses da empresa.

O acesso ao Data Center será realizado apenas por funcionários autorizados, mediante controle de acesso eletrônico. O acesso de terceiros deverá ter o acompanhamento de um funcionário autorizado da PLURAL que será o responsável por autorizar o acesso.

O acesso à rede interna somente será realizado através das estações de trabalho ou notebooks pertencentes ao patrimônio da PLURAL, esses equipamentos são controlados para eliminar possíveis riscos de vulnerabilidades, vírus e política de utilização de softwares.

O procedimento formal para cadastrado, alteração de departamento, função ou exclusão é realizado através da solicitação do RH.

Assim como para qualquer mudança no acesso aos Sistemas Corporativos o Gestor do Sistema deve ser comunicado das mudanças necessárias. O Gestor do Sistema é o responsável pela inclusão, exclusão e alteração de usuários e perfis de acesso nos Sistemas Corporativos da PLURAL, assegurando o acesso do usuário autorizado somente às informações necessárias a sua respectiva função e prevenindo o acesso não autorizado a sistemas de informação.

Para acesso aos equipamentos e sistemas aplicativos ligados à Rede da PLURAL, cada usuário deverá identificar-se através de sua única senha. A senha é de uso pessoal e intransferível.

Se houver necessidade de prestadores de serviços ou temporários acessarem a Rede, a área contratante deverá comunicar ao RH que solicitará à área de Tecnologia.

Para que haja maior segurança nas estações de trabalho, o usuário deverá observar as seguintes determinações:

- Toda vez que for se ausentar da sua mesa de trabalho, o usuário deverá, preferencialmente, bloquear sua estação da seguinte forma:
  - Pressionar, ao mesmo tempo, as teclas “CRTL+ALT+DEL” e
  - Clicar na opção “Bloquear computador”.

- A data e hora das estações de trabalho não poderão ser alteradas pelos usuários, pois elas estarão sincronizadas com os servidores.
- Qualquer componente de hardware do equipamento de cada usuário só poderá ser instalado, trocado ou removido pela área de Tecnologia. Os usuários somente poderão utilizar os softwares instalados pela área de Tecnologia, não podendo instalar novos, alterar ou remover os existentes.
- Os microcomputadores deverão ser desligados pelos usuários, após o seu expediente de trabalho, para a conservação física e lógica, bem como para prevenção, no caso de ocorrer problema elétrico ou na manutenção da Rede.

A área de Tecnologia (Administrador da Rede LAN e/ou seus prepostos) deverá efetuar o controle de acesso, de acordo com os privilégios definidos, bem como a manutenção do cadastro dos usuários através da informação da área de Recursos Humanos sobre as movimentações (desligamento e transferências) de funcionários.

Os logs de acesso somente poderão ser acessados pelo Administrador da Rede e/ou seus prepostos.

A área de Tecnologia deverá instalar em todos os equipamentos, antes de sua utilização pelo usuário, softwares de detecção e proteção contra "vírus" (vacinas), software de inventário e software de controle e restrição de alterações ao Sistema Operacional e controle de acesso a arquivos e pastas nas estações de trabalho.

8. Normas de Senha de Acesso

Toda senha é de caráter pessoal, secreta e intransferível. Cada usuário é inteiramente responsável pela guarda e utilização de sua senha, o compartilhamento será considerado como falta grave e passível de sanções disciplinares.

Neste caso, a área de Tecnologia efetuará o bloqueio do acesso e comunicará a diretoria. As senhas são um meio de validação da identidade do usuário para obtenção de acesso a rede ou a um sistema de informação ou serviço.

Para nenhuma finalidade é permitida a utilização de programas maliciosos para descobrir ou quebrar senhas de arquivos e programas.

A senha deverá ser alterada a cada 90 dias corridos, sendo que não poderá ser repetida nas próximas 5 alterações. Observar que o usuário poderá alterar a sua senha, a qualquer momento, não sendo necessário aguardar os 90 dias entre as trocas.

O usuário será bloqueado automaticamente após 5 tentativas inválidas de logon e a duração do bloqueio será de 15 minutos.

A formação da senha deverá ser efetuada pelo próprio usuário, sendo composta por no mínimo 6 caracteres alfanuméricos.

Para a formação da senha, o usuário deverá tomar alguns cuidados para que não seja facilmente identificada por terceiros, como por exemplo, não utilizar:

- Nomes de cônjuges,
- Nomes de filhos,
- Data de Nascimento,
- Anagramas (palavra ou frase formada pela transposição das letras de outra palavra ou frase, exemplo, Belisa (Isabel), Avalor (Álvaro), Arima (Maria)).
- Números de documentos pessoais,
- Nunca usar uma senha igual ao nome do usuário.

Após a formação da senha, ela deverá ser memorizada pelo usuário, não devendo ser impressa e nem anotada, muito menos divulgada a terceiros.

A área de Tecnologia não pode solicitar e não necessita de sua senha para realizar qualquer atendimento.

9. Normas de Utilização de Software

A PLURAL concede para seus funcionários, terceiros e estagiários juntamente com os servidores, desktops, notebooks e demais recursos disponíveis do seu patrimônio, a concessão de utilização de softwares, devidamente licenciados, para o desempenho de suas atividades.

Todo software utilizado pela PLURAL tem seu direito de uso devidamente licenciado de terceiros. Salvo formalmente autorizado por um fornecedor oficial, a PLURAL não tem o direito de reproduzir software e manuais em seu poder, com exceção à montagem de cópias de segurança (backup), sob responsabilidade da área de Tecnologia.

Com relação ao uso em redes ou em máquinas multiusuárias, os funcionários da PLURAL somente deverão usar o software de acordo com a licença acordada. O número de cópias simultaneamente em uso não poderá ultrapassar o contratado com o fornecedor.

A contratação de serviços correlatos à Tecnologia, sob qualquer pretexto, tem que ser previamente submetidas à análise dos departamentos Jurídico e de Tecnologia. Somente é permitida a utilização de softwares homologados e licenciados através da área de Tecnologia. Caso ocorra alguma necessidade de utilização de algum software que não esteja homologado, deverá ser solicitada a área de Tecnologia, onde todos os procedimentos de homologação e legalização serão realizados.

Fontes, imagens gráficas, programas “Free” como adobe, pkzip, Babylon, imposto de renda são considerados softwares e devem ser homologados e terem os direitos de uso autorizados pela área de Tecnologia.

A PLURAL reserva para si o direito de realizar inventários em seus ativos.

A área de Tecnologia é responsável por:

- Avaliar a necessidade de aquisição de softwares, bem como a sua compatibilidade.
- Proceder à instalação do software adquirido pela PLURAL.
- Efetuar a transferência de software entre áreas ou entre micros da mesma área.
- Manter em local apropriado e em segurança os discos originais e seus backups (cópias de segurança), bem como os respectivos manuais e contratos de cessão de uso.

- Acompanhar, juntamente com o usuário, o prestador de serviço, quando de atualizações de software/hardware, apresentações de novos aplicativos etc.

Considerando que a Lei no. 9.609, de 19/02/1998, disciplinou a proteção da propriedade intelectual sobre programas de computador, todos os funcionários deverão observar rigorosamente o disposto nesta lei, sob pena de incidirem nas sanções previstas na aludida norma federal, conforme abaixo:

- Detenção de 6 meses a 2 anos ou multa, se violar direitos de autor de programa de computador;
- Reclusão de 1 a 4 anos e multa, se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente, inclusive quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral;
- Pagamento de multa diária, estipulada pelo juiz, inclusive por perdas e danos pelos prejuízos causados.

Os funcionários da PLURAL que identificarem na empresa alguma irregularidade no uso de software ou na respectiva documentação, deverão notificar a área de Tecnologia.

De acordo com as leis brasileiras, reprodução ilegal de software é crime federal, com pena de até 05 anos de reclusão e multa de até duas mil vezes o preço de varejo de uma cópia do produto, para cada cópia ilegal encontrada (Lei nº 7.646/88).

10. Normas de Utilização de dispositivos móveis

A PLURAL disponibiliza a cada funcionário, terceiro e estagiário um equipamento para uso individual. De acordo com as funções de cada área, este equipamento pode ser um Desktop ou Notebook. Este equipamento pertence ao patrimônio da PLURAL e é expressamente proibido retirá-lo das dependências da empresa exceto aqueles destinados a esta finalidade.

Qualquer notebook / desktop pessoal ou de visitantes da empresa não poderá adentrar a rede corporativa da PLURAL. Toda mídia (Pen Drive, DVD, CD, disquete, etc.) de origem externa deve ser submetida à área de Tecnologia antes de ser conectado nos equipamentos.

O uso do e-mail através de Smartphone ou Webmail deve respeitar as mesmas normas de utilização do correio eletrônico corporativo.

A PLURAL não se responsabiliza por equipamentos celulares e smartphones particulares utilizados para acessos ao e-mail da corporação.

11. Normas de Gestão de Máquinas Servidoras

As diretrizes básicas para a gestão e utilização de Máquinas Servidoras são as seguintes:

O acesso lógico, ao ambiente ou serviços disponíveis em servidores, deve ser controlado e protegido. As autorizações podem ser revistas, confirmadas e registradas continuadamente. O responsável pela autorização ou confirmação da autorização será a Área de Tecnologia (Administrador da Rede LAN e/ou seus prepostos);

O horário das máquinas servidoras deve ser sincronizado para permitir o rastreamento de eventos;

Proteção lógica adicional (criptografia) pode ser adotada para evitar o acesso não autorizado às informações;

O Sistema Operacional, assim como outros softwares básicos instalados nas máquinas servidoras, deve receber atualizações críticas, de acordo com as recomendações dos fabricantes;

O acesso remoto às máquinas servidoras deve ser realizado adotando os mecanismos de segurança pré-definidos para evitar ameaças à integridade e sigilo do serviço;

Os procedimentos de cópia de segurança (backup) e de recuperação devem ser documentados, mantidos atualizados e regularmente testados, de modo a garantir a disponibilidade das informações;

A compra de máquinas servidoras será permitida desde que sejam atendidos todos os requisitos tecnológicos, de segurança e de integridade. Portanto, é imprescindível que haja o parecer técnico da Área de Tecnologia da Informação.

12. Normas de Administração do Ambiente de Rede

O ambiente de rede é controlado pela Área de Tecnologia da Informação – Administração de Rede.

As diretrizes para a administração de rede são as seguintes:

Componentes críticos da rede local devem ser mantidos em salas protegidas e com acesso físico e lógico controlado;

A configuração de todos os ativos de processamento deve ser averiguada quando da sua instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes à configuração padrão que se encontram nesses ativos em sua primeira ativação. Serviços vulneráveis devem receber nível de proteção adicional;

O acesso lógico aos recursos da rede local deve ser realizado por meio de sistema de controle de acesso. O acesso será concedido e mantido pela Área de Tecnologia da Informação - Administração da Rede, baseado nas responsabilidades e tarefas de cada usuário;

A conexão com outros ambientes de rede, quando houver, e alterações internas na sua topologia e configuração devem ser formalmente documentadas e mantidas, de forma a permitir registro histórico;

Devem ser adotadas proteções físicas adicionais para os recursos de rede considerados críticos. Proteção lógica adicional deve ser adotada para evitar o acesso não autorizado às informações;

Devem ser observadas as questões envolvendo propriedade intelectual quando da cópia de software ou arquivos de outras localidades;

Informações sigilosas, corporativas ou que possam causar prejuízo à Instituição possuirão proteção adequada, para viabilizar o envio para outras redes;

Todo serviço de rede não explicitamente autorizado será bloqueado ou desabilitado;

Mecanismos de segurança baseados em sistemas de proteção de acesso (firewall) deverão ser utilizados para proteger as transações entre redes externas e a rede interna da Instituição;

Deverão ser implantadas ferramentas de bloqueio para inibir invasão da rede local.

13. Normas de Utilização de Estações de Trabalho

Com referência às estações de trabalho devem ser adotadas as seguintes regras:

Devem ser adotadas medidas de segurança lógica referentes ao combate a vírus, backup, controle de acesso e uso de software não autorizado;

As informações armazenadas em meios eletrônicos devem ser protegidas contra danos, furtos ou roubos, sendo adotados procedimentos de backup;

O acesso às informações atenderá aos requisitos de segurança, considerando o ambiente e forma de uso do equipamento (uso pessoal ou coletivo);

Os usuários da Área de Tecnologia da Informação devem utilizar apenas softwares licenciados pelo fabricante nos equipamentos da Instituição;

A impressão de documentos sigilosos deve ser feita sob supervisão do responsável;

Os relatórios impressos devem ser protegidos contra perda, reprodução e uso não autorizado.

14. Classificação da Informação

É necessário classificar a informação de acordo com sua importância, objetivando minimizar riscos para a PLURAL, quer no que se refere à divulgação de dados confidenciais dos clientes quer de caráter estratégico. Esta classificação deve ser revisada periodicamente pelo Gestor da Informação possibilitando um melhor controle.

Os níveis abaixo indicam os critérios que devem ser observados para a correta classificação das informações e as medidas de proteção aplicáveis na PLURAL:

Uso interno – neste nível de classificação, as informações devem ser acessíveis apenas a funcionários e a prestadores de serviços (terceiros), exemplo: Circulares internas, lista de telefones;

Uso público – informações de uso público podem ser divulgadas sem causar nenhum impacto, exemplo: lista de produtos comercializados;

Uso confidencial – são classificadas como de uso confidencial as informações cuja disseminação, acesso e divulgação a pessoas não autorizadas podem causar grandes impactos, exemplo: folha de pagamento dos funcionários (acessível apenas a área de GHRSA – Gestão Humana e Recursos Sócio Ambientais).

A PLURAL disponibiliza estrutura de diretórios que permite aos usuários realizarem uma correta classificação da informação e preservação em termos de confidencialidade, disponibilidade e integridade.

Esta estrutura tem por finalidade tornar simples a organização de pastas e arquivos, permitindo que o usuário consiga armazenar e disponibilizar a informação dependendo da classificação exigida.

A correta classificação da informação possibilitará a proteção dos ativos informacionais da PLURAL e o usuário como conhecedor das características e exigências do negócio, terá nesta estrutura recursos para implementação das políticas de segurança e a classificação da informação.

A PLURAL possui estrutura de pastas por departamento com níveis de permissões aplicadas que garantem a segurança no armazenamento e a segregação dos dados entre os usuários, nesta estrutura há disponíveis pastas que permitem o compartilhamento de dados entre departamentos com níveis de permissão bastante restritivos.

Mudanças na estrutura de diretórios são realizadas manualmente pelo Administrador da Rede e/ou prepostos.

15. Auditoria

Eventualmente poderão ser realizadas auditorias para verificação do grau de cumprimento dessa Política. A PLURAL poderá monitorar e/ou registrar o envio/recebimento de mensagens do correio eletrônico, o acesso à navegação de internet, os sistemas aplicativos e os softwares instalados nas estações de trabalho e equipamentos portáteis de qualquer usuário, respeitando a confidencialidade sobre o conteúdo dos itens auditados, mas dispensando, em razão da divulgação desta política, toda e qualquer notificação prévia ao emissor ou receptor da comunicação. São consideradas razões empresariais legítimas, mas não se limitam a:

- Identificar e diagnosticar problemas de hardware e software;
- Prevenir o uso incorreto do sistema;
- Investigar conduta imprópria ou ilegal, atividade não ética ou inadequada;
- Assegurar conformidade com os direitos de propriedade, licença e obrigações contratuais;
- Proteger os interesses empresariais da organização.

16. Considerações Finais

De acordo com a política de segurança da informação da PLURAL sempre que o usuário encontrar informações, aplicações ou procedimentos críticos sem o tratamento de segurança correto, deverá informar seu superior imediato para que sejam tomadas providências necessárias.

O não cumprimento das regras da política de segurança da informação da PLURAL acarretará em punição conforme previsto no código de ética e conduta.