PSI - Política de Segurança da Informação - Revisão atual: 06

1 Objetivo

Esta Política de Segurança da Informação é uma declaração formal do ACP Group acerca de seu compromisso com a proteção das informações, incluindo dados pessoais, de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todas as empresas que o integram, os seus colaboradores, fornecedores, clientes e Parceiros.

Seu objetivo é estabelecer as diretrizes a serem seguidas pelas partes envolvidas no que diz respeito à adoção de procedimentos, requisitos legais e práticas aplicadas, visando manter o alinhamento e a integração entre a estratégia organizacional e a Segurança da Informação, a Proteção de Dados e a privacidade dos titulares de dados pessoais, bem como as recomendações dos Órgãos Reguladores, disseminando a importância e induzindo a melhoria contínua, promovendo a proteção das informações sensíveis, propondo normas para o processo de gestão da Segurança da Informação.

Preservando as informações quanto à:

- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;
- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
- Privacidade: garantia de que os dados pessoais apenas sejam tratados de forma transparente, adequada e nos estritos limites de sua necessidade para o alcance de propósitos expressos e legítimos.

1.1 Aplicações

As diretrizes aqui estabelecidas devem ser seguidas pelo ACP Group, por todas as empresas que o integram, por todos os seus colaboradores, prestadores de serviço, clientes e parceiros onde se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a todas as partes interessadas de que os documentos, ambientes, sistemas, computadores e redes da empresa podem ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de todos manter-se atualizado em relação a este documento, aos procedimentos e normas relacionadas.

2 Uso dos Serviços de Infraestrutura.

A utilização de recursos de informática deve ser feita de forma a preservar a segurança e integridade das informações e, bem como a proteção de dados e a privacidade dos titulares, e, para tanto, o usuário tem ciência da presente política e se obriga a segui-la com todo o rigor.

O acesso ao recurso e informações, incluindo dados pessoais, disponibilizado para o usuário limita-se ao estritamente necessário e indispensável ao exercício de suas atividades.

2.1 Posto de Trabalho

É disponibilizado para cada profissional, um posto de trabalho, composto de equipamentos e softwares, para que este desempenhe suas funções. O usuário é responsável pelas informações armazenadas na sua estação de trabalho. Para isso deve seguir diretrizes e práticas de segurança de Informação para minimizar e evitar a exposição de informações consideradas sensíveis para a organização, clientes e parceiros.

- Terminantemente proibida a cópia de qualquer informação em mídia externa que não seja para uso exclusivo da empresa ou de seus clientes;
- Ao se ausentar de seu posto de trabalho, o usuário deve bloquear a sua sessão na estação de trabalho de forma a proteger as informações que estão sob seu poder.
- É terminantemente proibido ao usuário abrir, alterar ou trocar por conta própria a configuração e/ou os equipamentos de seu posto de trabalho;
- As estações de trabalho possuem ferramentas de proteção contra software malicioso e é dever do usuário mantê-lo atualizado, assim como as atualizações do sistema operacional. Deverão ser obedecidas as normas de estilo (papel de parede, tela de login, proteção de tela, cores e estilos) definidas, não podendo colocar fotos ou outras imagens que não sejam as determinadas pela (DTI);
- Na sede ou filiais, a movimentação de qualquer equipamento de TIC é realizada somente com o auxílio da Coordenação de Infraestrutura (CIN), sendo necessário abrir uma solicitação de serviço. O controle da movimentação dos bens é feito pela (Coordenação Administrativa) CADM. As estações de trabalho estão sujeitas à inspeção da CIN e devem ser disponibilizadas para este fim, pelos respectivos usuários, quando solicitado;
- Os documentos impressos e mídias eletrônicas, quando não estiverem em uso, não devem estar expostos sobre a mesa. Sempre manter em local seguro;
- Os documentos com Informações considerados Confidenciais, devem ser guardados em local restrito e com controle de acesso;
- Anotações, recados e lembretes não devem ser deixados amostra;
- Não anotar informações confidenciais em quadros brancos, Post-it, etc;
- Não guardar documentos restrito e confidencial em local de fácil acesso;
- Destruir os documentos impressos antes de jogar fora;
- Não imprimir documentos apenas para ler;
- Sempre fazer impressão segura, quando não for possível ao imprimir retirar o documento imediatamente da impressora;
- Sempre que sair de frente do computador manter a tela Bloqueada;
- Manter na tela do computador (Área de trabalho) apenas os documentos que estão sendo utilizados;
- Manter qualquer tipo de caderno, agenda, bloco de notas etc. Utilizado para anotações em gaveta trancada;
- Durante o trabalho obrigatório o uso do crachá de identificação;
- Caso perder crachá ou cartão de acesso comunicar imediatamente;

- Desligar as estações de trabalho ao final do expediente, garantindo a desconexão de serviços de rede ou aplicações;
- Trancar o local de trabalho ao deixa-lo, não deixar o local de trabalho aberto sem que haja um profissional presente;
- O Uso, ou conversão, de dados pessoais em formato físico apenas será admissível quando estritamente necessário à finalidade almejada.

A informação é um grande patrimônio para a organização vamos protegê-la.

2.2 Equipamentos Pessoais e de Terceiros.

Equipamentos de uso pessoal, como notebooks, tablets e smartphones, devem ter o uso restrito às funções desempenhadas pelo profissional na empresa.

O Usuário encontra-se ciente que, caso faça uso de equipamento próprio para a prestação de serviço, episódica ou sistematicamente, este equipamento restará configurado como equipamento de trabalho, devendo ser utilizado única e exclusivamente para esta finalidade, e, findo o seu vínculo com o ACP Group, ou uma das empresas que o componham, esse equipamento poderá ser requerido para o adequado descarte de informações, incluindo dados pessoais, que sejam de propriedade, e/ou de responsabilidade, do grupo ou de uma das empresas que o compõe, sendo o Usuário responsável por danos decorrentes de sua não colaboração com a realização do dito descarte.

Na sede e filiais, a utilização de equipamentos não pertencentes à empresa deve ser pré-autorizada pela CIN, registrado na CADM e seguir os padrões de segurança interna, sendo necessário identificá-los de forma diferenciada. É expressamente proibido conectar qualquer equipamento à rede de dados e telefonia, sem a prévia autorização da CIN. A autorização deverá ser solicitada pelo superior imediato e liberada mediante registro de data limite da autorização, com respectiva justificativa. Caso a data limite de acesso do equipamento não seja informada, adota-se o prazo padrão de liberação por **24 horas**.

2.2.1 Diretrizes quanto ao uso de Mídias Removíveis e da porta USB

Mídias removíveis são dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Disquete, Pen Drive, cartão de memória, HDs portáteis, telefones celulares, entre outros.

A porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais. Tal vulnerabilidade não pode ser contida com firewalls já que os dispositivos são acoplados aos equipamentos pelos próprios funcionários da empresa.

Para minimizar os riscos de exposição e perda de dados sensíveis mantidos pela empresa e reduzir os riscos de proliferação de malwares nos computadores, a transferência de informações para dispositivos removíveis é bloqueada nos equipamentos da empresa.

A liberação das portas USB dos desktops e notebooks é feita somente se o uso for justificado e aprovado pelo líder do solicitante. O dispositivo USB deve ser preferencialmente adquirido pela empresa, está criptografado e protegido por senha, o dispositivo só é liberado para utilização na sua diretoria. Para notebooks da DEX esta liberação é efetuada por padrão.

Mesmo em equipamentos liberados o tráfego de dados entre as unidades USB e os computadores é monitorado através relatórios providos pelo sistema de gerenciamento, auditorias internas e externas, e validações feitas pelo comitê de segurança da informação e compliance

Sugere-se que, no ambiente da empresa se dê preferência ao armazenamento nos diretórios da rede e repositório.

Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos de informação, cabendo a eles as punições citadas neste documento.

2.3 Correio Eletrônico Corporativo

O serviço de correio eletrônico corporativo (e-mail) permite que os profissionais possuam uma caixa postal de forma que possam enviar e receber mensagens internas e/ou externas, cientes de que as mesmas e seu conteúdo são de propriedade exclusiva do ACP Group e das empresas que o compõem, podendo, seu uso, ser monitorado para verificar se a sua utilização está sendo feita de forma adequada, bem como para fins de investigação interna. Como forma de reduzir os riscos à segurança da informação, todos os e-mail são criptografados.

O profissional deve utilizar e divulgar seu endereço de e-mail corporativo exclusivamente para mensagens relacionadas às suas atividades na empresa, não devendo em hipótese alguma, utilizá-lo para cadastros em sites de compras, relacionamentos, dentre outros.

Por se tratar de uma ferramenta de trabalho, as mensagens recebidas e/ou enviadas pelo profissional podem ser auditadas sem necessidade de conhecimento e/ou autorização prévia e, havendo constatação de uso inadequado poderão ser apagados de forma definitiva.

A caixa postal do e-mail corporativo do profissional é mantida em servidor da empresa, ocupando o espaço máximo a ele designado e poderá ser consultada a partir de sua estação de trabalho ou através do webmail em qualquer local que tenha acesso à internet, com cuidado para evitar armazenamento de assuntos ou informações desnecessárias e/ou irrelevantes, principalmente aquelas com arquivos anexos.

O cliente de e-mails homologado para a utilização nas dependências da empresa é o Microsoft Outlook, não sendo permitido redirecionamento ou outras formas de acesso, exceto o webmail.

Devem ser obedecidas as normas de estilo (assinatura, tamanho e fonte) de e-mail, conforme orientado no sistema Doc, tamanho máximo da caixa postal (1Gb) e arquivos anexos (20Mb por mensagem), de forma a não bloquear o envio e recebimento de mensagens na caixa postal.

A assinatura dos emails seguem conforme indicado no link a seguir: [[http://doc.quali4tic.com.br/doku.php?id=processos_da_qualidade:assinaturas_de_email|Padrão de Email Corporativo]].

2.4 Compartilhamento de Arquivos (Sede e Filiais)

O servidor de arquivos permite ao profissional alocado na sede e filiais da empresa manter arquivos de uso comum em diretórios no servidor de rede, conforme as permissões (leitura e/ou gravação) estabelecidas para seu perfil.

Todas as pastas e arquivos com dados e documentos, sejam armazenados no servidor ou nas estações, estarão sujeitos à auditoria, sendo que aqueles de conteúdo considerado inadequado, quando não expressamente autorizados, poderão ser apagados de forma definitiva.

Em hipótese alguma a empresa se responsabilizará pela perda, corrupção ou uso indevido de informações e/ou dados particulares do usuário, eventualmente armazenados na sua estação de trabalho.

É proibida a utilização dos servidores para armazenamento de fotos, vídeos, músicas ou outros dados de caráter particular.

2.5 Transferência de Informações

A transferência de informações formais através de recursos eletrônicos pode ser realizada por meio do e-mail corporativo, ou em caso de arquivos através do servidor de FTP (ftp://ftp.quali4tic.com.br).

O acesso ao FTP é controlado através de login e senha específico para setor e cada cliente. O cliente tem permissão apenas para ler os dados e não gravar. O acesso de gravação é concedido ao setor nas pastas dos clientes.

No caso de transferência de informações internamente, na sede, é usada a área temporária da rede (Unidade Y:\), acessada através de login e senha dos profissionais. Essa área é limpa de forma automática todas as noites às 22h, garantindo que os dados que disponibilizados e que não foram apagados não estarão mais disponíveis no dia seguinte.

As informações, classificadas como confidencias, e que precisam ser compartilhadas entre os setores específicos, internamente, devem ser realizadas através de pastas específicas, destinadas às áreas, com controle de acesso no diretório de arquivos comuns (Unidade V:\).

Todos os profissionais são orientados a não compartilhar arquivos confidenciais na área temporária da rede e estão cientes de sua responsabilidade sob qualquer arquivo nela disponibilizado.

2.5.1 Armazenamento na Nuvem

O armazenamento na nuvem utilizando recurso (OneDrive) homologado previamente pelo líder/superior do solicitante é permitida pela organização e os acessos são controlados pela CIN.

Quando necessário a utilização de outra ferramenta para armazenamento na nuvem que não seja homologada pela empresa, esta deve ser previamente autorizada pelo líder/superior do solicitante, contendo justificativa plausível.

Para o uso de armazenamento na nuvem (OneDrive) deve ser autorizado pelo superior do solicitante, ciente que:

- A transição de dados através da nuvem deve levar em consideração os cuidados previstos no item 2.5 desta PSI;
- A responsabilidade pelo vazamento de informação na transição de arquivos na nuvem é inteiramente do usuário; e
- É permanentemente proibida a transição de arquivos confidenciais pela nuvem.

Após fim do contrato profissional, todos os acessos serão revogados e é necessário que líder/superior do profissional solicite para a CIN o backup dos dados, pois com a exclusão da conta do profissional o conteúdo online poderá ser perdido.

2.6 Impressão (Sede e Filiais)

As impressoras instaladas nas estações de trabalho dos profissionais alocados na sede e filiais da empresa são para uso exclusivamente relacionado às suas atividades. Preferencialmente, o usuário deve utilizar impressoras departamentais conectadas diretamente à rede, evitando o uso da impressora geral, salvo se não houver impressora no departamento.

Deverão ser tomadas precauções para que os documentos enviados à impressora geral não sejam lá esquecidos e fiquem acessíveis a outras pessoas.

As impressões poderão ser auditadas e controladas pela CIN.

2.7 Telefonia (Sede e Filiais)

O serviço de telefonia permite ao profissional alocado na sede e filiais da empresa efetuar ligações telefônicas para números fixos e celulares locais, DDD e DDI, conforme o nível de acesso autorizado pelas diretorias.

Eventualmente, as Diretorias poderão solicitar à CADM a disponibilização de linhas de telefonia celular para uso individual de um profissional ou Setor, dentro dos planos corporativos mantidos com as operadoras de telefonia e gerenciados pela CADM.

Sendo o serviço de telefonia da empresa considerado essencialmente uma ferramenta de trabalho, em casos de suspeitas de ameaças à segurança, ou de qualquer tipo de fraude ou ainda desvio de conduta profissional, a empresa poderá, a critério da sua Diretoria, efetuar gravações dos ramais telefônicos, sem necessidade de aviso prévio ao usuário, sendo que o conteúdo dessas gravações será considerado sigiloso, não devendo ser divulgado externamente pela empresa, a menos que requisitado por decisão judicial.

2.8 Mensageiro Instantâneo (Sede e Filiais)

O uso de mensageiros instantâneos externos (Skype, WhatsAPPWeb, Google Hangout, ICQ) é permitido, desde que aprovado previamente pelo líder/superior do solicitante.

A manutenção da lista de contatos nos mensageiros instantâneos será de exclusiva responsabilidade do usuário.

A utilização de mensageiros instantâneos deve ser exclusivamente para uso profissional de acordo com as funções do profissional na empresa, devendo, sempre que possível, ser evitado o compartilhamento de dados pessoais por esses meios.

O download de arquivos nos mensageiros instantâneos será controlado, com eventuais limitações com relação ao tipo e tamanho de arquivo.

A utilização de mensageiros instantâneos poderá ser monitorada pela CIN, independente de aviso ao usuário, de forma a detectar quaisquer abusos ou riscos à segurança de TIC em função do uso indevido por parte do usuário.

Aos profissionais alocados na sede e filiais da empresa é disponibilizado um mensageiro interno para facilitar a comunicação dos profissionais.

2.9 Acesso à Internet (Sede e Filiais)

O serviço de acesso à internet permite que o usuário acesse sites da WEB em apoio às suas atividades na empresa. O acesso a sites de notícias, busca, bancários ou webmail, mesmo que para uso particular, são permitidos, desde que não atrapalhe a produtividade e o desempenho das atividades do profissional.

Por ser a internet primordialmente uma ferramenta de trabalho, todos os acessos são monitorados e registrados, podendo ser negados nos sites de conteúdo inadequado e/ou que tragam risco à segurança de TIC.

São expressamente proibidos acessos a sites constantes na black list dos sistemas de segurança da empresa ou ainda que possam implicar em ações criminais tais como:

- Sites de conteúdo pornográfico;
- Sites de conteúdo racista;
- Sites que façam apologia ao uso de drogas e violência;
- Sites de jogos;
- Acesso a salas de bate-papo fora dos interesses da empresa;
- Comércio eletrônico fora dos interesses da empresa;
- Propaganda proposital de vírus eletrônico.

O acesso a Redes Sociais é liberado apenas para o setor responsável pela comunicação organizacional.

São controlados e eventualmente bloqueados pela CIN os downloads de arquivos suspeitos e/ou com extensões de multimídia que provoquem alto consumo de recursos de rede, exceto quando previamente autorizados.

2.10 Uso de Software (Sede e Filiais)

Nas estações de trabalho da empresa estão instalados somente softwares homologados. A CIN é o setor responsável por homologar os novos softwares ou novas versões de software e, posteriormente, permitir a sua instalação A instalação de qualquer outro software deverá ser solicitada à CIN, via solicitação de serviço no sistema SOL.

É vedado o uso, ou instalação, de software, programas ou aplicativos em violação as normas vigentes sobre propriedade intelectual ou de fabricante não confiável. Não será permitida, em

hipótese alguma, a instalação, cópia ou distribuição de programas que sejam de propriedade da empresa para instalação em qualquer computador que não conste no seu patrimônio.

A mídia original e a licença de todo o software homologado e adquirido pela empresa ficará armazenado na Biblioteca de Mídia Definitiva, sob a responsabilidade da área CIN, sendo disponibilizada quando necessário apenas uma cópia.

2.11 Acesso Remoto

O serviço de acesso remoto, através de uma rede privada virtual (VPN), permite que o USUÁRIO, portando de uma chave de acesso, utilize, remotamente e de forma segura via WEB, funções tais como:

- Acesso a sistemas corporativos que possuam interface WEB via navegador de internet;
- Download e upload de arquivos no servidor de rede;
- Acesso a sistemas corporativos que não possuam interface WEB via software cliente específico;

A chave de acesso é solicitada pelo líder/coordenador/diretor do profissional. A permissão e liberação de chave para acesso remoto é previamente analisada pela CIN.

Após criada a chave, ela é enviada para o e-mail ao profissional juntamente com os arquivo de conexão. Cabe a ele a responsabilidade por guarda e segurança da chave de acesso. Semestralmente a CIN faz a revogação e a geração novas chaves de VPN, comunicando os profissionais. Caso haja perda da chave ou suspeita de cópia não autorizada é informado à CIN para que esta faça a revogação do acesso.

O acesso remoto de fornecedores para manutenção, suporte e ou atualização de qualquer sistema utilizado internamente, não utilizará a VPN interna, sendo realizado diretamente sob a Internet através de softwares previamente autorizados e deverá ser informado e acompanhado pela CIN durante todo o seu período de atividade.

Cabe a CIN, durante o acompanhamento, cessar o acesso remoto ao identificar atividades irregulares não previstas no escopo do atendimento solicitado, destacadamente o acesso, ou qualquer outra forma de tratamento, de dados pessoais que não sejam necessários à finalidade pretendida.

Não é autorizado, sob nenhum aspecto, a realização de acesso remoto à rede interna sem que haja o acompanhamento pela CIN.

3 Segurança Corporativa.

Dados Pessoais, aqui entendido como qualquer informação que permita identificar, direta ou indiretamente, uma pessoa natural.

3.1 Proteção da Informação

A informação pode estar presente em diversas formas, tais como: sistemas de informação, diretórios de rede, bancos de dados, mídia impressa, magnética ou ótica, dispositivos eletrônicos, equipamentos portáteis, microfilmes e até mesmo por meio da comunicação oral.

Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada.

O profissional que receber as informações confidenciais deverá mantê-las e resguardá-las em caráter sigiloso, bem como limitar seu acesso, controlar quaisquer cópias de documentos, dados e reproduções que porventura sejam extraídas da mesma. Nenhuma das informações confidenciais pode ser repassada para terceiros sem consentimento do remetente ou área proprietária da informação.

O uso ou revelação indevida de uma informação confidencial deverá ser registrada prontamente num incidente de segurança da informação.

São exemplos de informações confidenciais:

- Informações de profissionais que devem ser protegidas por obrigatoriedade legal, incluindo dados cadastrais (CPF, RG etc.);
- Informações sobre produtos e serviços que revelem vantagens competitivas da empresa frente ao mercado;
- Todo o material estratégico da empresa (material impresso, armazenado em sistemas, em mensagens eletrônicas ou mesmo na forma de conhecimento de negócio da pessoa);
- Todos os tipos de senhas a sistemas, redes, estações de trabalho e outras informações utilizadas na autenticação de identidades. Estas informações são também pessoais e intransferíveis.

Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não.

Ao usar uma impressora coletiva, recolher o documento impresso imediatamente.

Não devem ser discutidos ou comentados assuntos confidenciais em locais públicos, ou por meio de mensagens de texto. Observar também quando houver outras pessoas no ambiente de trabalho que não sejam pertencentes ao departamento.

3.2 Autenticação e Uso da Senha

O usuário é o único responsável pelo sigilo de sua senha, e, por conseguinte, por todas as informações que a mesma lhe proporciona, podendo alterá-la a qualquer momento no sistema de Registro de Horas ou, em caso de esquecimento, devendo solicitar à Coordenação Desenvolvimento Humano Organizacional (CDHO) a renovação da mesma.

A senha de acesso ao e-mail é alterada diretamente no webmail e não é sincronizada automaticamente com a dos outros ambientes e sistemas.

Para usuários que utilizam dispositivos móveis como notebooks, pendrives e/ou hd's externos a senha ou chave de criptografia, BitLocker, gerada no momento da sua implementação, pela CIN, é transmitida através do e-mail corporativo, apenas para o usuário, com as instruções de utilização.

Em hipótese alguma o usuário poderá divulgar e/ou compartilhar sua senha.

O acesso do usuário aos serviços de infraestrutura e/ou aos sistemas de informação poderá ser modificado, bloqueado ou cancelado nas seguintes situações:

- Rescisão ou término contratual do usuário com a empresa;
- Transferência de local de trabalho do usuário;
- O usuário não mais possuir a necessidade de utilização dos serviços de infraestrutura e/ou dos sistemas de informação;
- O usuário não mais possuir a necessidade de utilização ou acesso a determinadas informações, destacadamente dados pessoais;
- Após ter o acesso negado por consecutivas tentativas sem sucesso;
- Em caso de suspeita de violação ou ameaças à segurança;
- Por decisão da Diretoria da empresa.

Em caso de bloqueio, o desbloqueio de acesso deverá ser solicitado pelo usuário, com prévia autorização de seu líder, através de procedimento formal junto à CIN, que deliberará caso a caso a decisão.

O usuário ao definir sua senha deverá observar as regras específicas de segurança estabelecidas:

- Tamanho mínimo da senha: 8 caracteres (a senha não deve possuir menos que 8 caracteres);

- A senha deve ser complexa, ou seja, não conter partes significativas do nome da conta do usuário ou o nome todo;

- A senha deve conter caracteres de 3 (três) das 4 (quatro) categorias abaixo:

- Caracteres maiúsculos (A até Z);
- Caracteres minúsculos (a até z);
- Caracteres numéricos (0 até 9);
- Caracteres especiais (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/).

- Ser alterada a cada 90 (noventa) dias.

3.3 Acesso Físico (Sede e Filiais)

O acesso físico às dependências da empresa é controlado através de diretrizes conforme o Controle de Acesso da empresa. O CPD da empresa é uma área de acesso restrito e permanece trancado. A chave fica sob responsabilidade da equipe de suporte, sendo que uma cópia de segurança permanece na CADM.

3.4 Acesso ao Código-Fonte de Programas

O controle de acesso código-fonte de sistemas é de responsabilidade da Gerência de Configuração. O acesso é fornecido baseado nas atividades da equipe do projeto e da permissão de acesso aos diretórios necessários à função exercida pelo profissional. Toda essa administração é realizada pelo Gerente de Configuração com o apoio do Líder e quando aplicável, do Gerente do Projeto, utilizando a ferramenta Subversion, que tem a função de controlar versão e gerenciar arquivos, diretórios e os responsáveis pelas modificações realizadas neles ao longo do tempo.

3.5 Backup (Sede e Filiais)

As unidades e diretórios de rede da empresa possuem cópia de segurança, gravadas diariamente.

As mídias (ou dispositivos de armazenamento) ficam armazenadas em um local protegido e fora da empresa. Seu transporte é feito em caixa hermética de forma a proteger a fita contra mudanças bruscas de temperatura, poeira, umidade, corrosão e impacto.

O tempo de vida e uso das mídias de backup é monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

As mídias defeituosas ou inservíveis são destruídas de forma a impossibilitar a recuperação dos dados por terceiros.

As solicitações de gravação ou restauração de dados deverão ser feitas através de chamado no sistema SOL e serão atendidas conforme prazos acordados com a Coordenação de Infraestrutura (CIN).

3.6 Descarte

O processo de eliminação da informação é tão ou mais importante que a sua geração ou armazenamento. Por isso, o descarte de mídias ou eliminação de conteúdos de informação sensível ou sigilosa deve atender aos seguintes procedimentos para o descarte seguro:

- Dispositivos de armazenamento (CDs, DVDs, discos rígidos, memórias "flash" e outros meios de armazenamento) devem ser descartados através da destruição física ou sobrescritos de forma segura;
- Documentos impressos que contenham informações pessoais, financeiras ou outros dados importantes para a empresa devem ser destruídos e não podem ser reutilizados.
- Tratando-se de descarte de mídia contendo dados pessoais, devem ser tomadas as medidas técnicas adequadas para assegurar que os dados pessoais não sejam acessíveis;
- Tratando-se de descarte de mídia contendo dados pessoais, o descarte deve ser registrado e documentado de forma adequada.

4 Registros de Incidentes de Segurança

Um incidente de segurança da informação é indicado por um ou mais eventos de que caracterizem violação ou não cumprimento de qualquer item desta política de segurança de informação, ou das demais normas, políticas e procedimentos que a complementem, dentre as quais a Política de Proteção de Dados.

Os incidentes relacionados a riscos à segurança poderão ser denunciados através da ouvidoria (pelo formulário de contato no site da empresa), de forma confidencial, ou através de registro no sistema SOL. Todos os incidentes relatados terão sua causa investigada, serão adequadamente documentados e, quando adequado, serão notificadas as partes interessadas.

Nos casos em que houver violação desta Política ou das demais Normas de Segurança da Informação, sanções contratuais, administrativas e/ou legais poderão ser adotadas, podendo culminar com o desligamento e responsabilização cível e/ou criminal, se aplicável.

O não cumprimento das normas estabelecidas neste documento, seja isolada ou cumulativamente, poderá causar, de acordo com a infração cometida, as seguintes punições:

Comunicação de descumprimento: Será encaminhado ao funcionário, por e-mail, comunicado informando o descumprimento da norma, com a indicação precisa da violação praticada. Cópia desse comunicado permanecerá arquivada junto à Coordenação Desenvolvimento Humano Organizacional na respectiva pasta do funcionário;

Advertência ou suspensão: A pena de advertência ou suspensão será aplicada, por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade;

Demissão por justa causa: Nas hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho.

5 Responsabilidades

É dever das partes interessadas manter-se atualizado em relação a esta PSI, aos procedimentos e normas relacionadas, bem como comprometer-se com a melhoria contínua do Sistema de Segurança da Informação, buscando orientação do seu líder, da CIN ou da CQC sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações e recursos.