PSI – Política da Segurança da Informação

Diretrizes e Normas Administrativas

Autor:	TI COOPED
Versão do documento:	V_1.0
Nome do Documento:	Política de Segurança da Informação
Localização Interna	A definir
Localização Externa	A definir
Data:	10/08/2021

DEPARTAMENTO: TECNOLOGIA DA INFORMAÇÃO – COOPED-CE	**EMISSÃO:** 10/08/2021
NOME: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	**REVISÃO:** 10/08/2021

COOPED-CE
Cooperativa dos
Pediatras do Ceará

Sumário

INTRODUÇÃO 4
OBJETIVO 4
CONCEITO DE SEGURANÇA DA INFORMAÇÃO 5
ABRANGÊNCIA 5
CLASSIFICAÇÃO DA INFORMAÇÃO 6
APROVAÇÃO E REVISÃO 6
RESPONSABILIDADES ESPECÍFICAS 7
E-MAILS 8
INTERNET 10
MESA LIMPA E TELA LIMPA 11
SENHAS 13
TERCEIROS 14
BACKUP 15
PROCESSO DISCIPLINAR 16
DISPOSIÇÕES FINAIS 17

INTRODUÇÃO

A informação é um ativo de grande valor para a COOPED-CE, devendo ser adequadamente utilizada e protegida contra ameaças e riscos. A adoção de políticas e diretrizes visa garantir a qualidade e disponibilidade das informações. As políticas e diretrizes devem ser prioridade constante na COOPED-CE, reduzindo-se os riscos de falhas, danos e prejuízos que possam comprometer a imagem e os objetivos da cooperativa.

A informação pode ser manipulada de diversas formas, ou seja, por meio de arquivos eletrônicos, mensagens eletrônicas, internet, bancos de dados, meio impresso, verbalmente, mídias de áudio e de vídeo etc.

Por princípio, a segurança da informação deve abranger três aspectos básicos, destacados a seguir:

Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

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.

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

OBJETIVO

A Política de Segurança da Informação é uma declaração formal da COOPED-CE acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores/terceiros.

Estabelecer diretrizes que permitam aos colaboradores, fornecedores e cooperados da COOPED-CE seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

CONCEITO DE SEGURANÇA DA INFORMAÇÃO

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela COOPED-CE pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

A COOPED-CE, por meio do Departamento de Tecnologia da Informação, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

A segurança das informações deve ser prioridade em todos os processos implantados, e projetada eficazmente nos novos negócios da corporação.

Para acesso a qualquer informação da COOPED-CE, deve-se considerar, por princípio, que tudo o que não é expressamente permitido é proibido, e que o direito de acesso deve ser concedido somente quando existir real necessidade do acesso a informação.

São considerados ativos de informação: processos de negócios, base de dados, arquivos, sistemas internos, sistemas externos, backup, diagrama de rede, códigos fonte de sistemas, documentação de sistemas, manuais, análise de impacto de negócios, planos de continuidade etc.).

Cada colaborador que tenha acesso ou manipule informações armazenadas ou mantidas pela COOPED-CE é considerado responsável pela segurança dos ativos e informações que estejam sob sua custódia, assim como por todos os atos executados sob sua chancela, conforme identificações de acesso.

As pessoas contratadas, a qualquer título, devem ser treinadas e mantidas atualizadas para o pleno exercício de suas funções, bem como sobre as políticas, normas e procedimentos de segurança.

ABRANGÊNCIA

Todos os funcionários, diretores, prestadores de serviços, consultores, auditores, temporários, fornecedores, parceiros diversos e demais contratados que estejam a serviço e disponibilizam de ativos corporativos da COOPED-CE suas Unidades, subsidiárias e/ou coligadas.

CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade do Gerente/Supervisor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com os critérios a seguir:

Pública: É uma informação da COOPED-CE ou de seus cooperados com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.

Interna: É uma informação da COOPED-CE que ela não tem interesse em divulgar, onde o acesso por parte de indivíduos externos à empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da Organização, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os empregados e prestadores de serviços da COOPED-CE.

Confidencial: É uma informação crítica para os negócios da COOPED-CE ou de seus cooperados. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais à COOPED-CE ou aos seus cooperados. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por empregados, cooperados e/ou fornecedores.

Restrita: É toda informação que pode ser acessada somente por usuários da COOPED-CE explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

APROVAÇÃO E REVISÃO

Os documentos integrantes da estrutura normativa da Segurança da Informação deverão ser aprovados e revisados conforme os seguintes critérios:

Política:

a. Nível de Aprovação: Diretoria

b. Periodicidade de Revisão: 02 anos

Normas:

a. Nível de Aprovação: Diretoria responsável pela área envolvida

b. Periodicidade de Revisão: Anual **Controle Técnico**:

a. Nível de Aprovação: Departamento Tecnologia da Informação – COOPED-CE

b. Periodicidade de Revisão: Semestral

RESPONSABILIDADES ESPECÍFICAS

Dos Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a COOPED-CE e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Dos Colaboradores em Regime de Exceção (Temporários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Segurança da Informação.

A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

Dos Gestores de Pessoas e/ou Processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da COOPED-CE.

Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da COOPED-CE.

Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI, bem como aos termos da Norma Educacional.

Cabe a todos os colaboradores:

- Cumprir fielmente a Política de Segurança da Informação da COOPED-CE;
- Buscar orientação do superior hierárquico ou gerente do departamento em caso de dúvidas relacionadas à segurança da informação;
- Assinar ciência e o aceite da Política e das Diretrizes de Segurança da Informação, bem como assumir responsabilidade por seu cumprimento;
- Assegurar que as informações não sejam acessadas, modificadas, destruídas ou divulgadas sem autorização de seus devidos proprietários;
- Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para desempenho de suas funções corporativas;
- Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual;
- Comunicar imediatamente ao Gerente do próprio Departamento ou Departamento de Tecnologia da Informação, qualquer descumprimento ou violação desta Política.

E-MAILS

Tal como telefone, o e-mail também é forma de comunicação de uso da COOPED-CE, cujo objetivo é tornar suas atividades mais rápidas e fáceis. O e-mail também caracteriza um compromisso com terceiros, sejam eles clientes ou prestadores de serviço, portanto, o uso desta ferramenta deve ser feito de forma cautelosa, profissional e com linguagem adequada.

Como se trata de ferramenta de trabalho de propriedade da COOPED-CE, a empresa se reserva do direito de rastrear, monitorar, gravar e inspecionar quaisquer informações transmitidas através de correspondência eletrônica, sem prévio aviso, com objetivo de evitar riscos decorrentes de ataques externos e do mau uso da ferramenta.

Os Colaboradores, com a aceitação dos termos e condições desta Política de Segurança da Informação, autorizam a COOPED-CE a acessar as informações transmitidas e recebidas através de suas contas de email, ficando cientes de que o uso indevido ou não autorizado os sujeitará a punições.

Recomendações sobre o uso do Correio Eletrônico (E-Mail)

É vedado o uso de sistemas webmail externo. O uso do correio eletrônico para envio e recepção de e-mail deverá ocorrer apenas através do correio eletrônico da COOPED-CE.

É proibido o uso do Correio Eletrônico para envio de mensagens que possam comprometer a imagem da empresa perante seus clientes e a comunidade em geral e que possam causar prejuízo moral e financeiro.

Evitar utilizar o e-mail da empresa para assuntos pessoais.

Assegurar a propriedade de todas as mensagens geradas internamente e/ou por meio de recursos de comunicação e definir o uso desses recursos como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividades de negócio e podendo ser monitorado por ser propriedade da empresa e até mesmo vistoriado por direitos de verificação e auditoria.

Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas: .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela área de TI.

Evite anexos pesados. O limite máximo de anexos é de 20MB por e-mail.

Não utilizar o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não reenviando e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/Symantec, criança desaparecida, criança doente, materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais, etc.

Utilizar o e-mail para comunicações oficiais internas, as quais não necessitem obrigatoriamente do meio físico escrito. Isto diminui custo com impressão e aumenta a agilidade na entrega e leitura do documento.

A utilização do e-mail/webmail da empresa fora do horário de trabalho para posições que possuam controle/reporte de jornada deve ser aprovado pelo responsável da área.

Todos os e-mails enviados, principalmente aqueles com arquivos anexados, devem ser rigorosamente checados e enviados com o máximo cuidado com relação ao destinatário para evitar que informações confidenciais ou de uso restrito se extraviem.

Não se deve cadastrar em sites de compras e entretenimentos o e-mail corporativo como contato.

INTERNET

O acesso à Internet é permitido a todos os colaboradores usuários de computador, com o objetivo de facilitar suas tarefas, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à empresa. Também é ofertada rede wifi com acesso exclusivo à internet, sem acesso aos servidores internos, tanto para colaboradores quanto para cooperados. Essa rede sem fio também é monitorada seguindo as mesmas diretrizes das redes de produção.

Todas as regras atuais da COOPED-CE visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a COOPED-CE, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A COOPED-CE, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e penalidades, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

Para uma utilização eficiente e produtiva algumas regras devem ser obedecidas:

- É proibido o acesso a sites ilegais ou não autorizados, tais como os relacionados a sexo, pornografia, pirataria, filmes, música, atividades de hacker e quaisquer outras

atividades ilegais. Estes exemplos não esgotam a lista de sites proibidos, portanto quaisquer dúvidas devem ser levadas ao conhecimento da área de TI - HelpDesk.;

- Fica proibido também o download de arquivos e programas não autorizados ou sem revisão e aprovação do Departamento de Tecnologia da Informação;
- É vedado também o acesso à sites de Corretoras, com o objetivo de efetuar operações de renda variável. A intenção desta política é evitar que vírus, cavalos de Tróia e outros programas indevidos, não licenciados e nocivos apareçam no ambiente de computação da COOPED-CE;
- Os acessos à Internet são controlados por um servidor de Proxy, que atribui uma autenticação a cada conexão feita pelo colaborador, gerando log's de acesso aos sites visitados. Esses log's dão origem a relatórios que são repassados aos gestores responsáveis de cada área para análise;
- Aliada a essa funcionalidade temos o controle de acesso aos sites não permitidos relatados anteriormente, impedindo que os mesmos sejam acessados. Quaisquer atividades que contrariem as regras de acesso à Internet ficarão sujeitas a penalidades;
- Quando observado por um associado a necessidade de acessar um determinado site que está previamente bloqueado, para fins profissionais, é possível solicitar o acesso a ele abrindo um chamando no Help Desk, informando endereço do site, justificativa para acessá-lo e período que precisa acessar;

Papéis e Responsabilidades

Usuário:

- Manter sigilo de suas credenciais de acesso ao dispositivo e sistemas disponibilizados;
- Comunicar imediatamente a área de informática em caso de roubo, furto ou substituição do dispositivo.

Área de Informática:

- Conceder o acesso à rede de dados da COOPED-CE;
- Revogar o acesso dos dispositivos móveis em caso de roubo, furto, substituição do equipamento ou demissão do usuário.

MESA LIMPA E TELA LIMPA

A política de mesa limpa e tela limpa refere-se a práticas relacionadas a assegurar que informações sensíveis, tanto em formato digital quanto físico, e ativos (notebooks, celulares, tablets, etc.) não sejam deixados desprotegidos em espaços de trabalho pessoais ou públicos

quando não estão em uso, ou quando alguém deixa sua área de trabalho, seja por um curto período de tempo ou ao final do dia. É utilizada para diretrizes e procedimentos que reduzam o risco de violação de segurança, da exposição desnecessária de informações consideradas sensíveis, fraudes e roubo de informações causadas por documentos deixados ou guardados de forma inadequada no ambiente de trabalho.

A política de mesas limpas e telas limpas deve considerar os seguintes itens:

- Os documentos em papéis e mídias eletrônicas não devem permanecer sobre a mesa desnecessariamente, devem ser armazenados em armários ou gavetas trancadas, quando não estiverem em uso, especialmente fora do horário do expediente;
- Informações sensíveis ou críticas para o negócio da organização devem ser trancadas em local separado e seguro (armários, por exemplo);
- Anotações, recados e lembretes não devem ser deixados amostra sobre a mesa ou colados em paredes, divisórias ou monitor do computador;
- Não anotar informações sensíveis em quadros brancos;
- Não guardar pastas com documentos sensíveis em prateleira de fácil acesso;
- Destruir os documentos impressos antes de jogá-los fora;
- Informações sensíveis ou confidenciais, quando impressas em local coletivo, devem ser retiradas da impressora imediatamente;
- Fotocopiadoras devem ser protegidas contra uso não autorizado;
- Devolver, o quanto antes possível, todos os documentos obtidos por empréstimos de outros departamentos, quando eles não são mais necessários;
- Computadores e terminais de computador e impressoras não devem ser deixados "logados", caso o usuário responsável não esteja presente;
- Nos computadores, utilizar um protetor de tela que solicite uma senha para acesso;
- Guardar agendas e cadernos de anotações numa gaveta trancada;
- Manter os pertences pessoais em gavetas ou armários trancados;
- Nunca deixar crachá de identificação ou chaves em qualquer lugar; mantenha-as junto a você;
- Notificar o pessoal da segurança imediatamente se seu crachá ou chaves sumirem;
- Nunca escrever senhas em lembretes e nem tente esconde-las no local de trabalho;
- Não deixe mídias, como CDs em sua estação de trabalho;
- Mesas e móveis deverão ser posicionados de forma que dados sensíveis não sejam visíveis de janelas ou corredores;
- Ao final do expediente, ou no caso de ausência prolongada do local de trabalho, limpar a mesa de trabalho, guardar os documentos, trancar as gavetas e armários, e desligar computador;
- Manter as gavetas e armários fechados e trancados e não deixar as chaves na fechadura.
- Não colocar ou comer refeições e lanches sobre a mesa;
- Não colocar copos de água, suco, refrigerante ou café sobre a mesa;

- Sempre limpar sua área de trabalho antes de ir para casa, garantindo adequada organização dos itens/objetos manipulados;
- Trancar o local de trabalho ao deixá-la, não deixar o local de trabalho aberto sem que haja um colaborador que trabalhe no local presente.

SENHAS

Uma senha serve para autenticar uma conta, é utilizada no processo de verificação da sua identidade, assegurando que você é realmente quem diz ser e que possui o direito de acessar o recurso em questão.

O acesso não autorizado de terceiros às suas senhas pode gerar os seguintes problemas:

- Utilização para fim de práticas ilegais;
- Utilização do computador de outros para promover ataques;
- Destruição de informações;
- Disseminação de spams;
- Furto de números de cartões de crédito e senhas de banco;
- Furto de informações salvas nas máquinas.

Regras para Criação/Alteração de senha

Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

Selecionar senhas de qualidade, que sejam de difícil adivinhação.

Utilizar senhas diferentes para cada local de acesso.

A periodicidade máxima para troca das senhas é 45 (quarenta e cinco) dias, não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 30 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Alterar senhas temporárias no primeiro acesso ao sistema.

O que não deve conter na senha

As senhas não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Entre as regras de criação de senhas, existe uma regra muito importante que é NÃO utilizar palavras do dicionário como código ('geladeira', por exemplo), pois existem softwares capazes de descobri-las, fazendo combinação e teste de palavras em diversos idiomas.

Cuidados com a senha

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.).

Alterar a senha sempre que existir qualquer suspeita do comprometimento dela, solicitando formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação.

Bloquear sempre o equipamento ao se ausentar (Ctrl + Alt + Del ou tecla Windows + L).

Certificar-se de que não está sendo observado enquanto utiliza suas senhas.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao Departamento de Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

Efetuar logout de qualquer sistema da instituição após o uso.

TERCEIROS

É missão e responsabilidade de cada terceirizado ou visitante, observar e seguir as políticas, padrões, procedimentos e orientações estabelecidas para o cumprimento da presente Política

de Segurança da Informação. É imprescindível que cada pessoa compreenda o papel da segurança da informação em suas atividades diárias.

Todas as atividades executadas por terceiros e demais colaboradores, devem observar a legislação vigente e a normatização de órgãos e entidades reguladoras, com relação à segurança da informação.

Equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio, nem devem ser conectados às redes de produção da Organização. Existe uma rede sem fio especialmente dedicada para esse público, cujo tráfego para a rede interna é bloqueado e que provê apenas acesso à internet. Isso evita propagação de vírus e pragas virtuais a partir destes dispositivos aos ativos da COOPED-CE.

BACKUP

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de backup" – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

A empresa responsável pela gestão dos sistemas de backup deve realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

Caso seja realizado backup no modelo off-line, sem replicação em nuvem, as mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT).

As mídias de backups históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de sala-cofre, distante no mínimo 10 quilômetros do Datacenter. Para backup no modelo online, deve-se respeitar a mesma distância mínima de 10 quilômetros entre as cópias.

Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade nos termos do Procedimento de Controle de Backup e Restore. Quaisquer atrasos na execução de backup ou

restore deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento de Controle de Mídias de Backup.

Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup.

Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

PROCESSO DISCIPLINAR

O descumprimento ou violação, pelo usuário, das regras previstas na Política de Segurança da Informação (PSI) poderá resultar em um processo disciplinar formal assegurando um tratamento justo e correto aos colaborares que cometeram violações de segurança da informação. Este processo deve dar uma resposta de forma gradual, que leve em consideração os seguintes fatores:

- Natureza e gravidade da violação;
- Impacto no negócio;
- Reincidência de violação;
- Participação em treinamento de conscientização de segurança;
- Termo de Responsabilidade e Confidencialidade;
- Legislações relevantes.

As violações das normas expressas nesta Política podem gerar ao colaborador, dependendo da gravidade da conduta, a aplicação de advertência verbal ou advertência por escrito ou suspensão ou até mesmo sua demissão por justa causa e eventuais processos criminais, se aplicáveis.

No que diz respeito a terceiros, fica a critério da COOPED-CE o procedimento a ser adotado que pode ser desde um aviso até o pedido de saída imediata das dependências da empresa.

Todos os colaboradores da COOPED-CE devem participar dos Programas de Educação e Conscientização de Segurança da Informação para assim reduzir o risco de erro humano em atividades cotidianas.

DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da COOPED-CE. Ou seja, qualquer incidente de segurança subentende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

A Política de Segurança da Informação da COOPED-CE foi aprovada pela Diretoria e deverá ser amplamente divulgada a todos os colaboradores.

Os controles e normas de Segurança da Informação devem ser divulgados às áreas diretamente relacionadas à sua aplicação.