POLITICA DE SEGURANÇA DA INFORMAÇÃO

1. Objetivo

A Política de Segurança da Informação possui por objetivo instituir diretrizes estratégicas, mecanismos e controles que visam garantir a proteção e confidencialidades aos dados, informações e recursos da empresa, seus colaboradores, clientes, parceiros, fornecedores e demais agentes envolvidos diretamente ou indiretamente.

2. Abrangência

A presente Política abrange todos os agentes de segurança da informação, quais sejam, colaboradores, terceiros e visitantes que possuem acesso à informações confidenciais, aos equipamentos computacionais ou ambientes controlados que necessitem de um *login* ou cartão de acesso, para que lhe sejam disponibilizados tais informações.

Essa política é aplicável tanto ao ambiente informatizado quanto aos meios convencionais de processamento, comunicação e armazenamento da informação.

As informações e dados precisam ser preservados observando três princípios básicos da Segurança da Informação:

- **Integridade:** a Informação deve ter seu conteúdo original mantido, sendo protegida contra alterações indevidas, seja de forma intencional ou acidental;
- **Confidencialidade**: somente pessoas devidamente autorizadas podem ter acesso às informações;
- **Disponibilidade**: o acesso à Informação deve ser garantido às pessoas autorizadas sempre que for necessário.

Toda violação ou desvio é investigado pela Diretoria e Comitê de Compliance para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

3. Responsabilidades

A responsabilidade em relação à segurança da informação deve ser comunicada no momento da contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso adequado dos ativos, com o objetivo de reduzir riscos. Para isso, assinam termo de responsabilidade (Anexo I).

É obrigação de cada colaborador manter-se atualizado quanto a este guia e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Área de TI, sempre que não estiver absolutamente seguro quanto ao uso da informação e/ou ativos e/ou sistemas de informação.

Todo e qualquer incidente que afete a segurança da informação deverá ser comunicado imediatamente à Área de TI.

A Política de Segurança deve ser implementada por meio da adoção de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

A empresa adota ferramentas, procedimentos e controles para reduzir a vulnerabilidade a incidentes e atender aos objetivos da presente política, dentre eles: a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra software maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.

O não cumprimento das Normas de Segurança da Informação acarretará em violação às regras internas da empresa.

4. Área de Tecnologia da Informação

Constitui responsabilidade da Área de Tecnologia da Informação configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos.

Garantir segurança especial para sistemas com acesso público, realizando guarda de evidências (*log)* que permitam a rastreabilidade para fins de auditoria ou investigação.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados à processos críticos e relevantes para a empresa.

Planejar, implementar, fornecere monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

A formalização de ações e processos relacionados à Área de TI deve ser seguida de modo a padronizar e documentar solicitações de: a) aquisição (*hardware, software,* serviços, etc); b) Desenvolvimento (projetos, sistemas,

aplicativos, programas, etc); c) Manutenção (programas, concessão de privilégios, sistemas, etc).

A solicitação deve ser enviada por e-mail para a Área de TI e esta deve registrar em documento padrão da área, no qual deve constar, o responsável pela solicitação e descrição.

5. Utilização de Computadores e Recursos Tecnológicos

Os equipamentos disponíveis aos colaboradores são de propriedade da organização, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da empresa, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelo setor responsável.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um responsável da Área de TI.

Não é permitido o armazenamento de arquivos pessoais e/ou não pertinentes ao negócio da organização (fotos, músicas, vídeos, etc), pois podem sobrecarregar os servidores. Caso identificada a existência desses arquivos, poderão ser excluídos definitivamente por meio de comunicação prévia.

Documentos imprescindíveis para as atividades dos colaboradores da empresa devem ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores, não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Cada colaborador possui acesso somente à pasta e informações de rede relacionadas ao seu setor de trabalho. O acesso às demais informações será fornecido pela Área de TI mediante solicitação formal por e-mail do gestor da área solicitante, que ficará responsável por eventuais incidentes.

Durante a utilização dos equipamentos, computadores e recursos de informática, algumas regras devem ser atendidas:

- Todos os computadores de uso individual devem possuir senha para restringir o acesso de colaboradores não autorizados.

- Os colaboradores devem informar ao departamento responsável qualquer identificação de dispositivo estranho conectado ao seu computador.

- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico designado pela Área de TI.

- Deve ser evitado o consumo de alimentos e bebidas na mesa de trabalho e próximo aos equipamentos, ou documentos.

Com o término da prestação de serviço, a solicitação para bloqueio de contas de acessos deve ser formalizada pelo Recursos Humanos logo após a

formalização da rescisão, mediante envio de e-mail para a Área de TI, que deverá providenciar o cancelamento das credenciais de acesso profissional.

Os trabalhos desenvolvidos ou elaborados pelo colaborador pertencem exclusivamente à empresa, não cabendo ao colaborador o direito de retirá-lo ou copiá-lo quando de seu desligamento.

6. Uso de Dispositivos Móveis

A empresa deseja facilitar a mobilidade e o fluxo de informações entre os seus colaboradores, razão pela qual permite que utilizem seus equipamentos portáteis.

Quando se utiliza “dispositivos móveis” entende-se como qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da empresa, ou aprovado e permitido por sua área de TI, como: smartphones, notebooks, tablets e pendrives.

Essa política traz critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

Na qualidade de proprietária dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário.

Todo colaborador, sempre que possível, deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel (se for o caso), bem como deverá manter os backups separados de seus dispositivos.

Todos os equipamentos utilizados para a atividade profissional deverá utilizar senhas de bloqueio automático (se possível).

O colaborador se responsabiliza em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da Área de T.I.

O uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venham causar à empresa ou a terceiros.

É permitido o uso de rede banda larga de locais conhecidos pelo colaborador, como sua casa, hotéis, fornecedores e clientes.

Para utilização de equipamentos que não são fornecidos pela empresa, será necessária solicitação, quando poderão não ser validados e autorizados para uso.

7. DataCenter

O servidor deve ser mantido fechado com trava eletrônica, com ambiente apropriado para o funcionamento, com controle de entrada, ar condicionado em constante funcionamento, câmeras de monitoramento e extintor de incêndio em local acessível.

O acesso ao Datacenter somente deverá ser feito por pessoas previamente autorizadas, visando a não interrupção dos serviços de servidor de arquivos, acesso à rede interna, acesso à internet e telefonia.

O acesso de visitantes ou terceiro somente será realizado com acompanhamento de um colaborador autorizado.

O Datacenter deve ser mantido limpo e organizado, não sendo permitida a entrada de nenhum tipo de alimento, bebida ou produto inflamável.

A entrada ou retirada de quaisquer equipamentos do Datacenter somente ocorrerá com a liberação de colaboradores previamente autorizados.

8. Uso do E-mail Corporativo

O uso do e-mail é para fins corporativos e relacionados às atividades do colaborador dentro da instituição, sendo vedada a utilização de outro endereço eletrônico para o exercício da atividade laboral. Assim, o uso desta ferramenta deve ser realizada de maneira cautelosa, profissional e com linguagem adequada.

Considerando que se trata de ferramenta de trabalho de propriedade da empresa, reserva-se o direito de rastrear, monitorar, gravar e inspecionar quaisquer informações transmitidas através de correspondência eletrônica, sem aviso prévio, com o objetivo de evitar riscos.

Os colaboradores manifestam ciência e aceitam essa Política, autorizando a empresa,a acessar as informações transmitidas e recebidas em suas através de suas contas de e-mail, ficando cientes de que o uso indevido ou não autorizado os sujeitará a punições.

Todos os e-mails enviados, principalmente aqueles contendo anexos, devem ser rigorosamente analisados e enviados com o máximo de zelo com relação ao destinatário para evitar que informações confidenciais ou de uso restrito se extraviem.

Todo e qualquer e-mail corporativo deverá sair com a seguinte comunicação:

> Este e-mail pode conter informações e documentos confidenciais e/ou protegidos por lei. Se você não for o efetivo destinatário, pedimos, por favor, que desconsidere completamente o seu conteúdo e os devolva ao seu remetente e os apague imediatamente, ficando proibida a sua cópia e/ou encaminhamento para terceiros.

Com relação ao uso do e-mail corporativo, algumas práticas são proibidas, sendo elas:

a) Perturbar outrem seja através de linguagem inadequada, alta frequência de mensagens ou excessivo tamanho de arquivos;
b) Enviar quantidade de mensagens excessivas em lote ou e-mails mal intencionados que, de acordo com a capacidade técnica da rede, seja prejudicial ou sobrecarregue intencionalmente usuários, site, servidor, etc.
c) Reenviar ou propagar, de qualquer forma, mensagens em cadeia ou pirâmides, independente da vontade do destinatário de receber tais mensagens;
d) Cadastrar em sites de compras ou newsletter utilizando o e-mail corporativo como contato.
e) Praticar crimes e infrações de qualquer natureza;
f) Forjar ou tentar forjar a identidade de outros usuários (por exemplo, usar o endereço de outro usuário para envio de e-mails).

Dica: desconfie de e-mails de fontes desconhecidas ou inesperadas, normalmente são e-mails falsos enviados com a intenção de prejudicar ou obter algum tipo de vantagem do destinatário (por exemplo, dados pessoais ou bancários). Ao receber um e-mail suspeito contate imediatamente a Área de Ti informando o fato para receber as devidas instruções. Em hipótese alguma abra o e-mail, mas caso aconteça, não clique em links, imagens ou execute o download de arquivos.

No caso de desligamento do colaborador da instituição, compete aos Recursos Humanos comunicarformalmente à Área de T.I, para que proceda com a retirada de acessos.

O colaborador não possui o direito de fazer cópias (backups) dos e-mails em caso de desligamento da instituição.

Deve-se evitar o acesso ao e-mail corporativo de maneira remota, sendo realizado somente quando imprescindível para a atividade, portanto, trata-se de excepcionalidade.

9. Senhas e Usuários

Os dispositivos de identificação e senhas protegem a identidade do colaborador, evitando e prevenindo que uma pessoa se faça passar por outra perante a organização e/ou terceiros.

A Área de TI é responsável pela criação da identidade lógica dos colaboradores na instituição (sistemas, rede de computadores).

Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deve trocar imediatamente a sua senha. É considerada uma senha segura quando contém 8 caracteres sendo letras maiúsculas, letras minúsculas e um caractere especial.

Todos os tipos de senhas a sistemas, redes, estações de trabalho e outras informações utilizadas na autenticação de identidades são pessoais e intransferíveis. Por segurança, não digite suas senhas ou usuários em máquinas de terceiros, especialmente fora da empresa.

10. Política de Mesa e Tela Limpa

Para garantir a confidencialidade e integridade das informações os colaboradores devem manter o ambiente de trabalho organizado, além do mais devem adotar as seguintes boas práticas:

- Informações impressas devem ser armazenadas corretamente ao se ausentar do seu posto de trabalho;

- Ao utilizar um recurso de uso comum, como sala de reuniões, é de responsabilidade do colaborador remover informações ou credenciais que foram utilizadas no mesmo;

- Os computadores de trabalho devem permanecer bloqueados (logoff) nos períodos de ausência do colaborador;

11. Boas práticas na comunicação verbal dentro e fora da empresa

Devem ser tomado cuidados ao tratar de assuntos relativos à empresa, dentro e fora do ambiente de trabalho, em locais públicos, ou próximo de visitantes, seja ao telefone ou com algum colega, ou mesmo fornecedor.

Assim, boas práticas devem ser tomadas, como abster-se de mencionar projetos e tratativas de assuntos confidenciais, fora da empresa ou próximos a pessoas desconhecidas, como visitantes.

Caso seja extremamente necessária a comunicação de informações confidenciais em ambientes públicos, fique atento as pessoas ao ambiente e tome todas as precauções necessárias para garantir a confidencialidade.

12. Política de Backups

A empresa adota rotinas sistemáticas de backup e guarda de informações, que são realizadas pela área técnica responsável. Cópias dos dados de produção, backup local e backup off-site devem ser produzidas, aplicando-se as melhores práticas de mercado com relação à segurança e proteção de dados.

As documentações físicas devem ser guardadas/arquivadas de forma segura, quer seja em ambiente interno ou externo, de acordo com o prazos previstos em lei para guarda e arquivamento do referido documento.

As cópias de segurança devem ser armazenadas em uma localidade remota, a uma distância suficiente para escapar de danos de um eventual desastre ocorrido no local principal, bem como as mídias devem ser regularmente testadas para garantir que são confiáveis no caso de uso emergencial.

13. Dispositivos de impressão, cópia e digitalização

Todos os ativos de informação devem ser devidamente guardados, especialmente documentos em papel ou mídias removíveis da empresa. Documentos não devem ser abandonados após a sua cópia, impressão ou utilização. Ao usar uma impressora coletiva, o usuário deverá recolher o documento impresso imediatamente.

As impressoras e seus respectivos suprimentos são de uso exclusivo para as atividades da empresa.

Os colaboradores devem recolher imediatamente suas impressões, sejam ela corretas ou falhas, quando deverão ser descartadas de maneira correta.

O descarte de impressões deve ser realizada somente após tornar ilegíveis as informações contidas nos documentos, não sendo autorizado a utilização das intituladas folhas rascunhos.

14. Notificação de Incidentes

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou suspeito, relacionado à segurança de sistemas e redes. Podemos citar como exemplos: tentativa de uso ou acesso não autorizado; tentativa de tornar serviços indisponíveis; desrespeito à política de segurança da informação.

Trata-se de dever do colaborador notificar a área de Compliance, sempre que verificar que uma atitude que considere abusiva ou com um incidente de segurança para que sejam tomadas as devidas ações, minimizando os impactos de ocorrência.