Bilt Contabilidade

Políticas de Segurança da Informação

Itajubá - MG - Brasil
Jul/2022

1. Objetivos

As políticas de segurança da informação apresentadas neste documento visam gerenciar as atividades de segurança, os procedimentos e diretrizes dos recursos de T.I. voltadas ao gerenciamento dos dados contábeis dos clientes.

Outro ponto buscado durante a elaboração deste documento é o alinhamento com políticas relacionadas à estruturação interna em atendimento LGPD, definidos por meio de Deliberações do Conselho Nacional de Contabilidade, que podem ser acessadas aqui.

A obtenção de segurança da informação é obtida através da implantação de controles, tecnologias, regras, processos e procedimentos, que poderão ser definidos neste documentos.

Este documento será compartilhado e divulgado para todos funcionários da empresa como parte do treinamento de segurança, de forma a garantir que todos possuam conhecimento acerca das suas responsabilidades e deveres sobre os dados mantidos pela empresa de contabilidade.

2. Abrangência

As políticas descritas neste documento deverão ser seguidas para qualquer nível hierárquico aplicável dentro da empresa. Assim, esta Política de Segurança de Informação aplica-se aos proprietários, empregados, assessores, terceirizados, estagiários, aprendizes, e demais colaboradores.

3. Atribuições e Responsabilidades

São atribuições dos Sócios-Proprietários:

- Garantir a existência de serviços que suportem a segurança da informação através do T.I.
- Solicitar revisões e alterações nas políticas de segurança de dados.
- Aprovar documentos sobre políticas de segurança de dados.

São atribuições dos prestadores de serviços de segurança de T.I.:

- Elaborar e revisar as políticas de segurança de dados de modo a atender os regulamentos externos (CFC, CRC/MG, LGPD).
- Implantar controles de segurança levantados por este documento.
- Realizar treinamentos na ocorrência de mudanças sobre controles de segurança.
- Produzir materiais sobre procedimentos facilitadores para assegurar a segurança de dados.
- Compartilhar as políticas definidas neste documento por toda estrutura organizacional.

São atribuições de TODOS funcionários aos quais esse documento abrange (Item 2):

- Conhecer e cumprir com as Políticas de Segurança da Informação.
- Reportar incidentes de não conformidade com este documento ao responsável pela prestação de serviços de segurança de T.I. ou

para algum sócio-proprietário, na ausência do responsável especializado na área.

4. Classificação de Informação

As informações atualmente mantidas pela empresa ou informações pessoais inseridas no dia-a-dia das pessoas componentes da empresa de contabilidade podem ser classificadas em 5 tipos: públicas, internas, restritas, confidenciais e secretas.

4.1. Informações Públicas: Toda informação de conhecimento público, que são disponibilizadas para os *stakeholders* por qualquer meio de comunicação.

4.2. Informações internas: Toda informação disponível para o acesso pelo funcionário, através dos meios oficiais de compartilhamento da empresa (servidor interno), para que possa ser realizado seu trabalho. As informações internas não podem ser divulgadas ou publicadas fora do servidor interno da empresa, com exceção do compartilhamento de dados de um cliente específico para os órgãos reguladores para prestação de contas, através dos portais governamentais.

4.3. Informações restritas: Toda informação disponível para somente uma parte específica da organização.

4.4. Informações confidenciais: Toda informação que só pode ser compartilhada entre pessoas autorizadas. A transmissão de informações confidenciais deverá ser feita através de meios de transmissão seguros, que garantam que as partes estejam autorizadas/autenticadas, exemplo: PDF protegido por senha.

4.5. Informações secretas: Informações com alto nível de sensibilidade, que não podem ser transmitidas sem autorização prévia de superiores diretos da estrutura organizacional. Exemplo: Senhas.

Para documentos físicos, a classificação da informação deve estar explicitada em lugar visível e de forma clara no documento, preferencialmente na primeira página.

Para documentos digitais armazenados no servidor interno compartilhado, a classificação de informação deve estar presente junto ao nome do documento, em caixa alta.

Quando um documento pode se enquadrar em mais de uma classificação, então é atribuída a classificação de nível mais alto para todo o documento.

5. Atividades e Deveres

Esta seção descreve os deveres para os funcionários aos quais esse documento abrange (Item 2) e os controles de segurança em vigor.

5.1. Responsabilidade sobre a classificação da informação

A atividade de classificação de informação, abordada no item 4, deve ser feita pelo funcionário que receber um documento, conforme esclarecimentos do item 4.

Se o documento for restrito ou confidencial, ele deverá ser encaminhado para o destinatário correto, que prosseguirá com o armazenamento correto e com a concessão da garantia de acesso.

5.2. Armazenamento de dados

Os dados relevantes para a realização do trabalho dos funcionários devem ser armazenados no servidor interno da empresa. Com exceção de dados públicos, nenhum outro dado (dentro da classificação do Item 4) pode ser mantido armazenado na máquina local.

5.3. Realização de backup

O backup dos dados deverá acontecer somente sobre os dados armazenados no servidor interno. Dados armazenados localmente nas estações de trabalho individuais não terão backups realizados pela equipe de T.I.

A tarefa de realização de backup deverá ser automatizada pelos fornecedores de serviços de T.I., não havendo necessidade de alocar algum funcionário para a realização da tarefa.

A periodicidade da realização do backup dos dados deverá ser acordada entre os prestadores de serviços de segurança de T.I. e os sócios-proprietários da empresa de contabilidade e será revista sempre que os sócios-proprietários acharem necessário. No momento, a periodicidade é diária.

5.4. Publicação de documentos

Todo documento contábil gerado de um cliente para prestação de contas junto aos órgãos governamentais regulamentadores devem ser enviados pelo responsável pelo documento, atribuído seguindo a norma 5.1. deste documento.

O envio de documentos só deverá ser feito através dos meios governamentais destinados para tal função. No caso de sites, o responsável deve identificar se o portal governamental onde ocorrerá a submissão de documentos é autêntico, verificando se o domínio é o correto e utiliza o protocolo HTTPS (que pode ser verificado na própria URL, no seu início - sites têm protocolo HTTP ou HTTPS). Se a submissão ocorrer por programas instalados na máquina do responsável, não é necessário a verificação de autenticidade, uma vez que os prestadores de serviços de T.I. já realizaram essa verificação.

5.5. Uso de ferramentas corporativas

A empresa se disponibiliza a fornecer condições tecnológicas adequadas para a realização de trabalho dos funcionários e está disposta a avaliar possíveis melhorias, quando solicitado.

O uso das ferramentas disponibilizadas deve seguir as diretrizes de segurança discorridas neste documento. No caso de algum item não estar em conformidade com a documentação apresentada é do dever so

funcionário informar ao responsável pela prestação de serviços de segurança de T.I. preferencialmente, ou para algum sócio-proprietário.

O uso das ferramentas disponibilizadas deve se ater ao máximo para o propósito real do trabalho, a realização de atividades pessoais sem fins corporativos deve ser realizada em dispositivos pessoais, utilizando de conexão de rede própria. Também não é permitido o uso de ferramentas corporativas como facilitador de práticas de atos ilícitos.

5.6. Email de trabalho

A empresa não possui um domínio de email corporativo, porém é necessário a criação de um email de uso exclusivo para o trabalho, usando o Gmail, usando o seguinte padrão: primeiro_nome.sobrenome.biltcontabilidade@gmail.com, exemplo: erika.souto.biltcontabilidade@gmail.com.

O uso do email criado deve ser de uso exclusivo para assuntos de trabalho e ao fim do contrato ele deve ser apagado, pelos prestadores de serviços de T.I.

5.7. Criação e distribuição de senhas de acesso

É recomendado que o funcionário crie senhas de acesso com mais de 8 dígitos, contendo ao menos uma letra maiúscula, uma minúscula, um número e um caractere especial.

Documentos classificados como confidenciais (item 4.4.) também têm a recomendação de seguir o padrão descrito acima.

Senhas não podem ser repetidas, independente do meio ao qual se aplica.

O aplicativo Bitwarden está disponível como possível ferramenta a ser adotada para a criação e o gerenciamento de senhas.

Quanto ao compartilhamento de senhas, é proibido que as senhas sejam compartilhadas, seja com pessoas dentro da empresa ou externas, com as seguintes exceções:

i) Caso se trate de um documento de uso compartilhado, que necessita de senha para acesso; então as pessoas autorizadas podem ficar cientes da senha do documento, que poderá ser compartilhada através dos emails de uso corporativo.

ii) Caso a transferência de responsabilidade do documento ocorra, por motivos de férias, desligamento de funcionário, distribuição de trabalho entre a equipe ou qualquer outro motivo que impossibilite que o responsável pelo documento continue mantendo a senha exclusivamente ao seu conhecimento.

5.8. Bloqueio de acesso ao dispositivo

Ao ser necessária a ausência do funcionário do ambiente físico de trabalho, onde é responsável por sua estação de trabalho, independente do tempo de ausência, o dispositivo deverá ser bloqueado usando o atalho Tecla do Windows + L.

5.9. Softwares

Todos os softwares necessários estarão disponíveis para o colaborador, desde o primeiro acesso à estação de trabalho. Caso algum

software não esteja presente, é necessário avisar aos prestadores de serviços de T.I. para que a questão seja resolvida.

Caso o funcionário deseje que algum software seja instalado em seu dispositivo, é necessário solicitar para os prestadores de serviços de T.I., junto da justificativa de uso do software. É de responsabilidade dos prestadores de serviços de T.I. assegurar que o software requerido não apresente riscos aos dados corporativos antes de liberar o uso e realizar a instalação.

As atualizações do sistema operacional (Windows) devem estar agendadas para ocorrerem de forma automática, sem que o usuário possa impedir o download da atualização. A instalação das atualizações devem acontecer preferencialmente fora do horário ativo de trabalho, o que também pode ser programado nativamente, como função do sistema operacional. A configuração do agendamento das atividades abordadas anteriormente é de responsabilidade dos prestadores de serviços de T.I.

As atualizações de softwares devem ocorrer conforme solicitado pelo próprio programa, ao detectar uma nova versão. Caso este tipo de verificação não seja uma função em algum dos softwares instalados, é necessário fazer a verificação manualmente. Define-se um período de uma semana entre checagens de atualização. A atualização só não deve ocorrer caso indicado pelos prestadores de serviços de T.I.

Manter os softwares atualizados é responsabilidade do funcionário que utiliza a estação de trabalho, sendo ele o responsável por autorizar que o processo automático de atualização ocorra. Caso ocorra algum incidente durante a atualização de software que não permita prosseguir com a atualização, é preciso solicitar um prestador de serviços de T.I. que assumirá a responsabilidade sobre o processo.

5.10. Antivírus

Atualmente a empresa conta com o uso comercial do antivírus Kaspersky em todas as estações de trabalho. Ele deverá ser mantido constantemente ligado e atualizado (conforme descrito no item 5.9.).

Caso o antivírus não esteja presente na máquina do funcionário, será de responsabilidade do mesmo solicitar que a instalação seja feita.

6. Violação de políticas

Caso alguma das políticas presentes neste documento sejam descumpridas, o trabalhador autor do descumprimento deverá passar por treinamento junto aos responsáveis adequados, para que a ocorrência não volte a se repetir.

A violação de políticas também deve gerar uma avaliação de toda a ação, por parte dos prestadores de serviços de segurança de T.I. para que sejam desenvolvidas formas para resolver a incoerência.

7. Versão do documento e vigência de políticas

Este documento é válido a partir da data de sua concepção, em 02 de julho de 2022.

Esta é a versão 1.0 do documento de Políticas de Segurança da Informação.

Futuras revisões irão atualizar, então ele não será o documento vigente. Assim, para garantir que o leitor tenha acesso a todas versões publicadas, as versões serão disponibilizadas na pasta “Documentação Geral”, na subpasta “Políticas de Segurança da Informação”, dentro do servidor da empresa.