INTRODUÇÃO: A presente política visa estabelecer regras visando a segurança do tratamento e proteção dos dados das pessoas naturais no âmbito da TEB, tendo por base a Lei Federal 13.709/2018. Baseia-se, também, na proteção à privacidade, liberdade de expressão, informação, opinião, comunicação, inviolabilidade da intimidade, honra e imagem, livre iniciativa, autodeterminação informativa, direitos do consumidor, direitos humanos, dignidade, exercício da cidadania pelas pessoas naturais, dentre outros fundamentos insculpidos na Constituição Federal e em outros diplomas legais.

1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A TEB reconhece que a informação é um ativo essencial para o negócio e, consequentemente, precisa criar mecanismos de proteção e controle para evitar perda ou mau uso desta informação.

O propósito desta política é definir os objetivos de segurança da informação da TEB e fornecer um enquadramento para gerenciamento de riscos de segurança da informação e controles apropriados.

2. ESCOPO/ ALCANCE

O escopo desta política abrange o armazenamento, acesso, transmissão e destruição de informação no negócio da TEB.

Esta política aplica-se a todos os colaboradores da TEB e outros com acesso a essas informações (independentemente da localização), bem como aplicativos, sistemas, equipamentos e instalações que criam, processam, transmitem, hospedam ou armazenam informações, sejam internas, de propriedade pessoal ou fornecidos por terceiros.

NOTA: dependendo dos termos contratuais assinados entre a TEB e o cliente, o colaborador assinalado para o serviço, estará obrigado a cumprir também com as Políticas de Segurança da Informação do cliente.

3. TERMOS E DEFINIÇÕES

Dados Pessoais: informação relacionada à pessoa natural identificada ou identificável, exemplos: Nome e sobrenome, Idade (Data de Nascimento), Endereço, E-mail, Endereço de IP, Cargo em exercício, Número de Identidade, CPF, RNE, Número de Passaporte, entre outros dados que possam identificar uma pessoa.

Dados Pessoais Sensíveis: segundo a Legislação Brasileira, refere-se aqueles dados pessoais com as seguintes caraterísticas: Convicção religiosa, Opinião Política, Filiação a sindicato ou a

CÓPIA CONTROLADA

organização de caráter religioso, filosófico ou político, Dados referentes a saúde ou a vida sexual, Dado genético ou biométrico, quando vinculado a uma Pessoa Física.

Ameaça: Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

Banco de Dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico, compreendendo todas as informações relacionadas a uma pessoa identificada ou identificável, direta ou indiretamente de indivíduo que esteja vivo. São os dados de identificação, como nome, RG, CPF, endereço, telefone, e-mail, endereço de IP, gênero, data e local de nascimento entre outros;

Backup: É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso de perda dos dados originais, o que pode envolver eventuais remoções acidentais ou dados corrompidos.

Cliente: é aquela Pessoa Física ou Jurídica que compra produtos e serviços da TEB.

Colaborador: refere-se ao membro da liderança, ao ocupante de funções gerenciais, empregado direto e indiretos, contratados, estagiários e jovens aprendizes que estão desenvolvendo atividades na TEB.

Cookies: são arquivos de informação que são armazenados no computador ou dispositivos móveis por meio do navegador de internet (browser). Estes arquivos permitem que, durante um período de tempo, um website “se lembre” das ações e preferências registradas em nome do Usuário.

- **Data Protection Officer (DPO):** também chamado de “Encarregado de Dados”, é o responsável por coordenar e por assegurar a conformidade com a Política de Proteção de Dados e requisitos legais/regulamentares locais aplicáveis, também, atua como o canal com os Titulares dos Dados e a Autoridade Nacional de Proteção de Dados ANPD, pelo e-mail tebroeck@tebmanutencao.com.br.

- Pelo **Erro:** equívoco; opinião ou julgamento que contraria a verdade.

Evento: incidente inesperado ou situação que altera a ordem normal da operação.

Informação Confidencial: toda informação que tem acesso restrito a terceiros, incluindo a certos colaboradores. Exemplo: dados da folha de pagamento dos Colaboradores, informação privilegiada num processo de Fusão ou Aquisição, Plano Estratégico.

CÓPIA CONTROLADA

Informação Pública: refere-se a todo conteúdo que o público em geral tem acesso, exemplos: campanha publicitária, informação no jornal ou mídia social, informação em cartórios e registros.

Informação de Uso Interno: toda aquela informação disponível para uso dos colaboradores da TEB para execução do seu trabalho rotineiro. Em consequência, a informação não é para uso público externo, exemplos: Políticas, Processos & Boas Práticas que não estejam publicadas na página de internet da TEB, e-mails corporativos, comunicados internos, qualquer documento utilizado ou material intelectual utilizado para tarefas diárias.

Titular dos Dados (Titular): pessoa natural ou indivíduo a quem se referem os dados pessoais que são objeto de tratamento.

4. PRINCÍPIOS GERAIS

Todos os colaboradores e usuários da rede e sistemas da TEB devem estar familiarizados com os princípios desta política e suas relacionadas relevantes para sua área de atuação. Também, são responsáveis de relatar incidentes, violações e sugestões para melhorias contínuas.

Cada colaborador da TEB deve seguir rigorosamente as seguintes medidas:

- Proteger ativos da informação crítica por meio de processos de avaliação de risco e implementação de mecanismos de controle;
- Definir processos e responsabilidades claras ao momento de manuseio de softwares e serviços de suporte, compartilhamentos de conteúdos;
- Promover consciência com respeito a Segurança da Informação dentro da TEB;
- Promover o reporte de eventos relacionados à segurança da informação para a devida tomada de medidas;
- Cumprir com os requerimentos legais e regulatórios aplicáveis e termos contratuais assinados.

5. CLASSIFICAÇÃO E TRATAMENTO DAS INFORMAÇÕES

Para garantir que as informações recebam um nível adequado de proteção, as seguintes regras de tratamento se aplicam por classificação:

CÓPIA CONTROLADA

Pública

Qualquer informação que a TEB compartilha com o público, na mídia social e no site da TEB, com aprovação.

- Verificar se a informação é segura para ser compartilhada ao público;
- Verificar se a informação não irá gerar algum impacto negativo no momento de publicar;
- Antes de publicar a informação, solicitar aprovação de algum membro do Comitê de Segurança da Informação;

Privada / Interna

Informação compartilhada entre dois ou mais indivíduos ou entre um grupo restrito que não contém informação sensível ou confidencial. Porém, a informação é restrita e terceiros poderão ser compartilhados se existe algum fundamento legal, exemplo: pedido especial de um Titular de Dados que a TEB coleta, auditorias.

- Caso houver necessidade de fornecer informação a um terceiro, formalize o envio por meio de mecanismos postais rastreáveis; evite compartilhar este tipo de informação por meio de e-mail, compartilhamento via nuvem;
- Envie a informação unicamente se existe alguma justificativa devidamente aprovada pelo DPO ou CEO;
- Solicite ao recipiente declarar a finalidade do uso da informação.
- Coloque manualmente uma marcação: “Informação Privada ou de uso Interno” e coloque-a em PDF caso a informação for compartilhada.
- Não deixar informação exposta.

Pessoal

Informação relacionada à pessoa física identificada ou identificável. Os dados pessoais incluem, mas não estão limitados a: nome, sobrenome, Idade (Data de Nascimento), endereço, e-mail, endereço de IP, cargo em exercício, número de Identidade: CPF, RNE, Número de Passaporte etc.

CÓPIA CONTROLADA

- Não deixar documentos expostos a terceiros;
- Coloque manualmente uma marcação: “Dado Pessoal ou Sensível” e coloque-a em PDF;
- Tratamentos de Dados Pessoais devem estar alinhados com a Política de Privacidade.

Sensível

Segundo a Legislação Brasileira, refere-se aqueles dados pessoais com as seguintes caraterísticas: Convicção religiosa, Opinião Política, Filiação a sindicato ou a organização de caráter religioso, filosófico ou político, Dados referentes a saúde ou a vida sexual, Dado genético ou biométrico, quando vinculado a uma Pessoa Física.

- Não deixar documentos expostos a terceiros;
- Coloque manualmente uma marcação: “Dados Pessoal ou Sensível” e coloque-a em PDF;
- Tratamento de Dados Sensíveis devem ter consentimento prévio e explícito por parte do Titular ou por requerimento legal ou regulatório.

Confidencial

Informações altamente restritas devendo manter sigilo, tanto escrito como verbal, ou, por qualquer outra forma, de todos os dados, informações científicas e técnicas e, sobre todos os materiais obtidos com sua participação, podendo incluir, mas não se limitando a: técnicas, desenhos, cópias, diagramas, modelos, fluxogramas, croquis, fotografias, programas de computador, discos, disquetes, pen drives, processos, projetos, arquivos em nuvem ou qualquer meio ou plataforma digital, dentre outros. Isso inclui:

- Informação de valor substancial ou crítica, ou rotulada como confidencial para efeitos legais.
- Também inclui, mas não limitado a informação privilegiada, documentação ou informação compartilhada com apenas algumas pessoas para promover certos propósitos.
- Informação Confidencial não deve ser compartilhada a menos que especificamente exigido e/ou aprovado pela diretoria.

CÓPIA CONTROLADA

- Criptografar a informação em caso de compartilhamento.
- Coloque manualmente uma marcação: “Informação Confidencial” e coloque- a em PDF;

6. DOCUMENTO DE USO INTERNO

Terceiros podem compartilhar informação com a TEB marcada com a sua classificação de informação. Toda informação recebida de terceiros deve ser tratada conforme os termos contratuais assinados com o proprietário da informação. Se o dono da informação não tiver definido nenhuma regra de tratamento, a informação deverá ser classificada conforme a pontos descrito acima.

7. USO DE EQUIPAMENTO

Dependendo da natureza do serviço oferecido, é disponibilizado equipamento tecnológico a cada um dos colaboradores contratados e/ou alocados para determinado cliente:

7.1 Equipamento da TEB ou alugado

Este equipamento pode ser de propriedade da TEB ou alugado por esta. Os colaboradores que recebem o equipamento por parte da TEB, deverão seguir as diretrizes desta política de segurança da informação. Entre os equipamentos que podem ser disponibilizados pela TEB estão: Desktop, Laptop (ou Notebook) e telefone celular;

7.2 Equipamento do Cliente

Este tipo de equipamento é de propriedade de certos clientes destinados a colaboradores que realizam um determinado serviço. Caso o colaborador receba algum equipamento do cliente, este deverá seguir os padrões de segurança da informação do cliente, além das práticas descritas nesta política. Entre os equipamentos que podem ser disponibilizados pelo cliente estão: Desktop, Laptop (ou Notebook) e telefone celular;

7.3 Equipamento do próprio colaborador

Este equipamento é de propriedade do profissional, e sua utilização é definida junto ao cliente e seu uso destinado única e exclusivamente as atividades profissionais. O colaborador deverá seguir os padrões de segurança da informação do cliente, além das práticas descritas nesta política.

CÓPIA CONTROLADA

Todos os colaboradores precisam seguir as seguintes diretrizes para o devido cuidado:

- É proibido todo e qualquer procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da equipe de suporte de TI da TEB ou do cliente se for aplicável.
- Todo colaborador deve adotar as devidas práticas de manutenção e uso devido de seus respetivos equipamentos fornecidos. Eles são os principais responsáveis pelo cuidado com o equipamento.
- Quando em deslocamento de carro, coloque o laptop no porta-malas ou em local não visível para evitar furtos.
- Quando em deslocamento por transporte público, garanta que a mochila / bolsa que o carregue esteja sempre com o usuário.
- Evite deslocamentos desnecessários com o laptop.
- Evite uso de laptops em lugares públicos e com alto movimento de pessoas.
- Sistemas e equipamentos devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. Caso houver suspeita de vírus ou problemas na funcionalidade, usuário deverá acionar o suporte técnico responsável da equipe de suporte de TI.
- Evitar guardar qualquer arquivo gravado localmente no equipamento (Exemplo no drive C:). Todo arquivo guardado no equipamento não tem garantia de backup
- O colaborador não deve copiar e/ou mover para os drives da rede arquivos pessoais ou que não pertençam à operação da TEB ou do cliente, exemplo: fotos, música, vídeos e outros arquivos.
- Informar imediatamente ao suporte de TI qualquer identificação de dispositivo desconhecido conectado ao seu equipamento;
- É vedado executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da empresa;
- Todos os computadores deverão ser protegidos por senha (bloqueados) quando não estiverem sendo utilizados. Sendo assim, sempre que o colaborador se ausentar de seu local de trabalho – mesmo que apenas por um minuto – deverá bloquear o seu computador (Basta pressionar a tecla “Windows + letra L” ou CTRL+ALT+DEL e selecionar a opção “Bloquear Computador” ou “Bloquear”), para garantir que ele esteja protegido de uso indevido durante a sua ausência;

CÓPIA CONTROLADA

- Caso os colaboradores trabalharem em locais da TEB ou do cliente, o acesso à estação de trabalho deverá ser encerrado no final do expediente, desligando o equipamento;
- O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas ou aplicativos que não tenham sido instalados ou autorizados por um técnico de suporte de TI da TEB;
- É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, fornecedores e clientes, observando se a mesma está protegida por senha;
- Em caso de perda, furto ou roubo de algum equipamento, o colaborador deverá abrir um Boletim Ocorrência (B.O.) e notificar imediatamente o seu gestor direto;
- O colaborador deverá utilizar senha/código de bloqueio nestes dispositivos para salvaguardar as informações contidas nele caso sejam roubados ou extraviados;
- Conduzir os negócios relacionados com o trabalho interno e clientes usando o bom senso em e-mails de trabalho e pesquisa na internet, por exemplo, garantir o conteúdo apropriado ao enviar e responder e-mails relacionados ao trabalho;
- Usar o e-mail e a navegação na Internet de forma a não interferir com as atividades e ou que não pare os serviços ou incorrer em custos adicionais para a TEB ou cliente;

Os Colaboradores têm totalmente proibida as seguintes atividades:

- Acesso não autorizado a outros equipamentos, servidores ou redes;
- Fazer declarações ou reivindicações falsas ou fraudulentas ao usar ativos da TEB ou de seus clientes;
- Utilizar o equipamento fornecido pela TEB ou cliente para vigiar, interceptar tráfico na rede de terceiros por meio de softwares ou ferramentas eletrônicas;
- Acessar, ver criar, promover ou distribuir qualquer material que: seja ilegal, antiético ou que cause constrangimento a terceiros., exemplo: material pornográfico, spam, mensagens que potencialmente tenham códigos maliciosos, malwares etc.
- Contornar ou reduzir quaisquer mecanismos de segurança da TEB, de seus parceiros ou clientes.
- Realizar qualquer tipo de intrusão ou técnicas invasivas, monitoramento ou varredura de rede fora do âmbito das funções autorizadas regulares.

NOTA: *Caso exista a situação em que o colaborador tenha que utilizar seu próprio equipamento para fornecimento de serviços, ele deverá contatar ao Departamento de TI para realizar o devido processo de homologação.*

CÓPIA CONTROLADA

Instalação, Atualização e Desinstalação

Qualquer tipo de instalação, desinstalação ou atualização no Hardware ou Software da TEB, deve ser devidamente realizado pelo departamento de TI da TEB ou com pessoal devidamente autorizado pela diretoria:

- Toda instalação, desinstalação ou atualização deve ser previamente homologada pela diretoria da TEB. Ao instalar atualizações de software, shareware, freeware, os usuários devem validar os custos e obter aprovação por escrito da diretoria da TEB. Contratos de licença devem ser cuidadosamente lidos e compreendidos antes de aceitar e prosseguir com a instalação.
- Instalar ou distribuir software pirata é proibido, incluindo o uso ou a compra de uma licença de usuário único, utilizando-o em vários computadores, da TEB ou de seus clientes.
- Caso necessite de um software ou hardware específico para desempenhar suas funções, por favor, alinhe com seu líder imediato a aquisição ou fale com a diretoria.

Acesso ao ambiente de sistemas e dados

Todo usuário deve ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O Colaborador assume a responsabilidade quanto ao sigilo da sua senha pessoal. É proibido o compartilhamento de senhas.

Por conseguinte, o colaborador dever ter os seguintes cuidados:

- A senha é de uso pessoal e não poderá ser fornecida a terceiros. Caso houver algum tipo de urgência, o colaborador deverá abrir um chamado junto ao Departamento de TI. Se a senha for compartilhada, troque-a imediatamente após finalizar o suporte;
- O colaborador deve utilizar uma senha forte de 8-12 caracteres. Também, a senha deverá conter números, letras (maiúsculas e minúsculas) e caracteres especiais (símbolos) e não deverá utilizar informações pessoais fáceis de serem obtidos como o nome, número de telefone ou data de nascimento;
- A senha deverá ser mudada a cada 90 dias e não poderá ser repetida;
- Utilizar um método próprio para lembrar-se da senha, de modo que ela não precise ser anotada em nenhum local, em hipótese alguma;

CÓPIA CONTROLADA

- Quanto ao acesso de plataforma de clientes, deve ser realizado exclusivamente por aqueles colaboradores autorizados, conforme a atividade que está sendo feita. Além desta política, o colaborador deve respeitar também as políticas de segurança da informação do cliente.

NOTA: *Caso o acesso do usuário seja bloqueado, o colaborador deverá contatar o departamento de TI da TEB para verificar o motivo do bloqueio e solicitar o desbloqueio.*

Acesso aos Servidores, Painéis Administrativos e Serviços

Os colaboradores de TI da TEB são os únicos que têm acesso aos servidores, painéis administrativos e serviços. Eles são responsáveis pela manutenção, atualização, promoção da segurança e disponibilidade dos acessos.

Quanto ao acesso a serviços em nuvem da TEB, deve ser realizado mediante login/senha individual, com autenticação de 2 fatores habilitada.

Uso de e-mails

O uso do correio eletrônico da TEB é para fins corporativos 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.

O colaborador deverá tomar as seguintes medidas:

- Não utilizar o correio eletrônico para mensagens pessoais e/ou que possam comprometer a imagem da empresa perante seus clientes e a comunidade em geral;
- O uso de e-mails externos como Hotmail, Gmail, Yahoo etc. só podem ser utilizados para fins pessoais. Neste sentido, não podem ser utilizados para realizar atividades da empresa. O uso do correio eletrônico para envio e recepção de e-mails deverá ocorrer apenas através do correio eletrônico da TEB;
- Manter sua caixa limpa, e-mails repetidos, propagandas, e-mails com muitos anexos podem comprometer a performance do seu Outlook e dificultar manutenções;
- Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertos: .bat, .exe, .src, .lnk, e .com, ou de quaisquer outros formatos alertados pelo suporte de TI da TEB;

CÓPIA CONTROLADA

- Não utilizar o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede e comprometer o domínio externo da TEB perante a outros serviços.

Navegação Web

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

A TEB 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 ações administrativas e penalidades decorrentes de processo civil e criminal, sendo que nesses casos a organização cooperará ativamente com as autoridades competentes.

É proibida a divulgação ou compartilhamento indevido de informações das áreas de negócio em listas de discussão, sites ou comunidades de relacionamento, salas de bate- papo ou chat, comunicadores instantâneos (exemplo Whatsapp, Messenger, Telegram) ou qualquer outra tecnologia relacionada que venha a surgir.

Os colaboradores não poderão utilizar os recursos da TEB para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de Tróia, spam, assédio, perturbação ou programas de controle de outros computadores.

Segurança Física

Os colaboradores devem proteger as instalações e equipamentos da TEB contra destruição, perda ou uso indevido, evitando acesso não autorizado a partes críticas das instalações. Implementação de medidas de segurança adequadas deve estar conforme com o nível de segurança da informação que consta em documentos, equipamentos e sua devida classificação.

Também os colaboradores devem tomar as seguintes medidas quanto ao resguardo da segurança física:

- Todos os colaboradores da TEB devem utilizar seu crachá no momento de acessar ou sair das instalações. NOTA: o crachá é de uso individual e não pode ser compartilhado.

CÓPIA CONTROLADA

- Em caso de perda do crachá, informe imediatamente ao RH para desativação imediata. Lembre-se que os crachás têm funcionalidade de chave de acesso.
- Em caso de terceiros, os visitantes deverão se apresentar e cadastrar na recepção do prédio. O visitante deverá estar sempre acompanhado desde o momento da entrada até a saída do prédio.
- Antes de convidar o visitante para uma sala de reunião, verifique a não existência de documentos ou informação sigilosa dentro da sala, exemplo: anotações, documentos em cima da mesa etc.
- Evite imprimir documentos para não deixar dados expostos, e quando for realmente necessário a impressão, classifique o documento como: Dados Pessoais, Dados Sensível e confidencial.

Mesa e Tela Limpa

Para evitar exposição desnecessária, documentos ou arquivos contendo informações sensíveis:

- Não devem ser deixados sobre a mesa de trabalho ou expostos em tela. Os usuários devem tomar cuidado com a exposição de informações sensíveis na tela de computadores em ambientes de circulação ou públicos;
- Toda documentação deve ser devidamente guardada em gavetas, armários ou locker com chave quando se ausentar da mesa;
- Documentos devem ser retirados da impressora, imediatamente após a impressão. Somente imprima um documento quando for extremamente necessário;
- Equipamentos e acessórios relacionados ao seu trabalho devem ser armazenados em local seguro e adequado, principalmente quando não estiverem em uso;
- Documentos ou mídias contendo informações confidenciais, e informação do cliente, devem ser picotados/fragmentados ou eliminados em um local aprovado pela TEB.
- No momento de concluir uma reunião presencial numa sala, verifique que a sala não tenha documentos na mesa e que dados na lousa ou em painéis estejam devidamente apagados

Teletrabalho ou Home Office

A TEB é uma empresa que se caracteriza por incentivar a prática de Teletrabalho (ou Home Office) já que gera flexibilidades rotineiras e contribui com uma melhor qualidade de vida dos colaboradores. Também para fins operacionais, funciona como uma excelente ferramenta de continuidade operacional já que não existe restrição nos locais onde o colaborador trabalha.

CÓPIA CONTROLADA

No entanto, existem riscos de vazamento da informação, se não forem tomados os devidos protocolos de segurança. Neste sentido, todo colaborador deve tomar as seguintes medidas:

- Procure um lugar com suficiente privacidade para trabalhar; evite lugares públicos onde a informação manipulada poderia estar em exposição de terceiros;
- Utilize rede de wifi seguros (com senha), que não comprometam a informação trabalhada;
- Pratique de forma remota o "Princípio de Mesa Limpa" tal como se estivesse trabalhando no escritório;
- O equipamento facilitado pela TEB para trabalhar é exclusivamente para realizar atividades de trabalho da empresa. As ferramentas não poderão ser emprestadas para terceiros nem podem ser utilizadas para outros fins.
- Desligue completamente o Computador quando não for usado;
- Tenha cuidado redobrado com o sigilo de suas senhas;
- Guarde o computador em um lugar seguro;
- Evite levar o computador a lugares público de alta exposição;
- Esteja preparado em como resolver possíveis incidentes de forma remota, exemplo: a quem chamar da TEB em caso de indisponibilidade ou falha do computador.

Reuniões à distância

A TEB dispõe de plataforma de vídeo colaboração para realização de reuniões à distância. Para tal recomendam-se as seguintes precauções:

- o Verifique exatamente os arquivos que serão compartilhados para que somente os assuntos necessários sejam usados via apresentação ou compartilhamento;
- o Prepare-se com antecedência, verificando os recursos de áudio, vídeo e conteúdo a serem utilizados.
- o Verifique que o lugar onde será realizada a vídeo conferência cumpre com mínimos parâmetros de privacidade;
- A Ferramenta adotada pela TEB é o Microsoft Teams

Uso de Sistemas de Redes Sociais

Atualmente, o acesso às redes sociais (exemplo: Facebook, LinkedIn) já faz parte do cotidiano de grande parte dos usuários da Internet. Entre outros motivos, são utilizadas como busca de

CÓPIA CONTROLADA

candidatos para vagas de emprego, pesquisas de opinião e mobilizações sociais. Porém vale ressaltar que possuem riscos e que alguns cuidados devem ser tomados para evitá-los.

Os principais riscos associados às redes sociais são:

- Invasão de privacidade;
- Furto de identidade;
- Invasão de perfil;
- Uso indevido de informações;
- Danos à imagem;
- Vazamento de informações;
- Recebimento de mensagens contendo códigos maliciosos;
- Instalação de programas maliciosos;
- Acesso à conteúdos impróprios ou ofensivos;

A concessão de acesso às redes sociais implica na utilização adequada, conforme recomendações abaixo:

- É proibido publicar assuntos que comprometam a imagem da TEB, seus clientes ou colaboradores;
- Respeitar a liberdade de expressão de cada indivíduo. Porém, é recomendado evitar publicar assuntos que provoquem conflitos ou mal-estar com terceiros;
- Não publicar informações do negócio sem prévia autorização por parte da diretoria da TEB.

Cabe ao usuário, manter o sigilo das informações da TEB, sendo de sua total e exclusiva responsabilidade qualquer informação compartilhada nas redes sociais. Ele deverá comunicar imediatamente ao suporte de TI qualquer situação que possa colocar em risco as informações da TEB.

Uso de Sistemas de Mensageria

O mau uso de mensagens (como Whatsapp e Telegram) pode deixar a TEB exposta. Seguem algumas medidas preventivas a serem adotadas:

CÓPIA CONTROLADA

- É proibido encaminhar qualquer tipo de informação confidencial por meio de sistemas de mensageria;
- Evite encaminhar qualquer tipo de informação a terceiros que pudesse comprometer a imagem da TEB;
- É proibido o uso de outros sistemas de mensageria público (exemplo: Telegram, Whatsapp, Messenger, Instagram) para as atividades rotineiras da TEB.

Engenharia Social

Engenharia social é a técnica de se aproveitar da boa-fé de pessoas para obter informações que possibilitem ou facilitem o acesso aos recursos computacionais de uma organização por parte de usuários não autorizados. Dentre as informações procuradas destacam-se as seguintes:

- Senhas de acesso;
- Listas de usuários;
- Tipos e versões de sistemas operacionais usados;
- Dados sigilosos sobre produtos e processos da organização.

Os contatos podem ser feitos de forma direta entre o engenheiro social e a vítima por meio de telefonemas e até mesmo pessoalmente, pois engenheiro social nem sempre é alguém desconhecido. Outra forma de contato é por centrais telefônicas parecidas com serviços de telemarketing onde um banco de dados com informações da pessoa e da empresa é criado e atualizado com base nas conversas destes contatos.

Também podem ser feitos por meio da utilização de softwares ou ferramentas para invadir, como por exemplo, vírus, cavalos de Tróia ou através de sites e e-mails falsos para assim obter informações desejadas. Podem ser mensagens que contenham avisos de premiações milionárias em loterias, ofertas de sociedade em grandes somas de dinheiro, heranças e negócios em outros países etc. O melhor a fazer é ignorar e apagar o e-mail imediatamente.

<u>Em seguida, algumas precauções a serem adotadas:</u>

- Sempre suspeite de qualquer Instituição ou pessoa física desconhecida solicitando fornecimento de informação confidencial, incluindo dados pessoais. Lembre-se que o Engenheiro Social utiliza mecanismo para gerar simpatia com a vítima, exemplo: ele

CÓPIA CONTROLADA

poderia se fazer passar por um representante de uma instituição, amigo de um colega ou familiar.

- Caso houver algum evento onde uma instituição específica solicita certa informação, informe para a pessoa que você retornará à ligação. Em vez de ligar para o número pelo qual a pessoa ligou, utilize os números oficiais da instituição;
- No momento de receber uma mensagem, revise o e-mail do remetente. Verifique que o e-mail corporativo coincide com a página de internet;
- Nunca forneça informação confidencial a um e-mail pessoal, exemplo: (gmail, hotmail, yahoo, etc).

Impressão de Documentos

Caso houver a necessidade de imprimir documentos com informação confidencial, o Colaborador deverá tomar as seguintes medidas:

- Guardar informação confidencial em pastas e resguardar em lugares seguros com chave;
- Se o documento que contém informação confidencial não for mais necessário, o colaborador deverá picotar ou rasgar da melhor forma possível para evitar qualquer tipo de vazamento;
- Está totalmente proibido fornecer qualquer tipo de documentação com informação confidencial, sem autorização previa pela diretoria da TEB.

Backup da Informação

Os sistemas da TEB contam com um cronograma de Backup automático por meio da equipe de TI. Caso houver algum sistema que não esteja no processo de backup automático da TEB, o administrador desse sistema deverá garantir o devido processo de backup frequentes e realizar testes de recuperação.

Qualquer atividade terceirizada, incluindo backup e restauração, devem ser acompanhadas pelo administrador do sistema, de acordo com os requisitos contratuais especificados.

Descarte Seguro de Equipamentos

Todo equipamento tecnológico contém Informação Confidencial na memória. Este equipamento, durante o transcurso do tempo, vai ficando cada vez mais obsoleto e em consequência, a TEB estaria obrigada a trocá-los por equipamento novo. Mas, antes de descartar qualquer equipamento tecnológico da TEB, a área de TI toma alguns passos para

CÓPIA CONTROLADA

apagar toda informação guardada. Neste sentido, todo equipamento a ser descartado, precisa passar antes pela área de TI para apagar toda a informação confidencial guardada.

8. RESPONSABILIDADES

Comitê de Segurança da Informação:

- Promover uma forte cultura, conforme os requisitos desta política e nos termos da legislação em vigor;
- Revisar, aprovar e atualizar esta política quando houver necessidade de alteração;
- Analisar os relatórios de teste e monitoramento baseado nos requerimentos desta política e garantir que as ações corretivas sejam tomadas para remediar qualquer tipo de deficiência;

Diretoria

- Administrar as ferramentas de trabalho fornecidas pela TEB; isto inclui manutenção, melhoras, mudanças, avaliações de risco, plano de contingência e treinamento dos usuários;
- Conceder acessos aos usuários de cada ferramenta, sempre respeitando a Classificação e tratamento das informações como descrito nesta política;
- Escalar qualquer evento que possa impactar a segurança da informação dentro da TEB.

Data Protection Officer (DPO) ou Encarregado de Dados

- Apoiar a implantação e a manutenção desta política e do cumprimento da legislação em vigor;
- Atender as solicitações e fiscalizações da ANPD;
- Ministrar treinamento e comunicação adequada dos itens desta política;
- Revisar e atuar em caso de ocorrência de exceção a esta política;

CÓPIA CONTROLADA

- Garantir que os mecanismos estejam em vigor para o registro e monitoramento apropriado de documentos relacionados a esta política;
- Informar e relatar incidentes relacionados a Proteção de Dados Pessoais ao Comitê de Segurança da Informação;
- Garantir que sejam tomadas as ações corretivas adequadas para remediar deficiências ou incidentes reportados com o apoio do Comitê de Segurança da Informação.

Diretor ou Gerente

- Criar canais de comunicação com colaboradores da TEB, para atender eventos que comprometam a segurança da informação;
- Implantar controles de Segurança da Informação;
- Coordenar o processo de descarte seguro de equipamento.

Assessoria Jurídica

- Interpretar leis e regulamentações aplicáveis a esta política;
- Oferecer orientação jurídica em relação às leis e regulamentações aplicáveis para os segmentos, áreas de suporte e controle;
- Garantir que as disposições das Políticas reflitam as determinações definidas nas leis e regulamentações aplicáveis.

Colaboradores

- Ler, entender e praticar esta política e outras relacionadas;
- Informar previamente ao DPO e ao superior imediato quando houver algum evento de não conformidade com a legislação vigente ou com os princípios desta política;
- Participar de forma periódica nos treinamentos preventivos;
- Questionar ou denunciar em caso de qualquer dúvida referente aos assuntos expostos;
- Relatar qualquer atividade suspeita, caso presenciar algum incidente;

CÓPIA CONTROLADA

- Não praticar qualquer ato que, embora não previsto em procedimentos de controle, seja contrário aos princípios desta Política, à legislação em vigor e aos princípios da ética, moral e bons costumes;
- Após o término contratual, devolver todos os ativos ou recursos fornecidos pela TEB durante o período de emprego ou serviço.

9. DÚVIDAS OU DENÚNCIAS

Em caso de dúvidas ou preocupação sobre como agir apropriadamente, ou se souber de alguma atividade que saia dos padrões éticos desta Política, sugerimos utilizar os seguintes canais:

Converse com o seu superior imediato: ele é o seu principal orientador. Sugerimos que, se não for lhe causar nenhum desconforto, você converse primeiro com o seu superior imediato. Ele poderá responder algumas das suas perguntas relacionadas ao dia a dia no trabalho e assuntos que envolvam esta política.

Contate a Ouvidoria: em caso de dúvidas, eventos relacionados a vazamento da informação ou requerimentos relacionados à Lei Geral de Proteção de Dados devem ser encaminhados via WhatsApp diretamente pelo número (15) 97404-9545 ou pelo WhatsApp disponível no site https://tebmanutencao.com.br/.

Não Retaliação: é proibida qualquer retaliação contra qualquer pessoa que, de boa-fé denuncie atividade ou comportamento que acredite ser ilegal, antiético ou uma violação de nossas políticas. A retaliação é contra os valores da TEB e não será tolerada.

10. EXCEÇÕES À ESTA POLITICA

As solicitações de práticas de atos que possam ser considerados como regras de exceção ou que, por não estarem bem definidos, necessitem de ajustes na aplicação e interpretação desta política, deverão ser feitas de forma escrita para o DPO da TEB. O pedido será analisado e, se aprovado pelo DPO, o Comitê de Segurança da Informação tomará a decisão final sobre a exceção e interpretação do fato e seu devido enquadramento.

11. SANÇÕES E PENALIDADES

A TEB não tolera de forma direta ou indireta nenhum tipo de prática antiética ou ilícita que viole os direitos de privacidade de cada Titular. Qualquer violação da Lei aplicável ou desta

CÓPIA CONTROLADA

política poderá causar graves danos à TEB e aos seus dirigentes e, como resultado, poderia ensejar a aplicação de penalidades disciplinares, multas, ações judiciais, processos administrativos, perda da licença e, ainda, a quebra de contrato com o Cliente.

Assim sendo, a violação da lei aplicável e/ou desta política por qualquer Colaborador ou empresa vinculada a TEB, ensejará sanções disciplinares, com a gradação da sanção conforme a infração praticada, a qual poderá resultar em advertência, demissão por justa causa, rescisão do contrato de fornecimento ou prestação de serviços e responsabilização pela indenização dos danos causados, inclusive com o infrator podendo ser levado às autoridades policiais e judiciais, se a infração for configurada como criminosa.

12. RETENÇÕES DE REGISTROS

A TEB deve documentar, arquivar e guardar os registros das atividades desenvolvidas e decisões proferidas em procedimentos administrativos ou judiciais decorrentes da aplicação desta Política, no prazo legal, em conformidade com a legislação aplicável da jurisdição onde opera.

13. ALTERAÇÕES DO DOCUMENTO

Data	Revisão	Alteração	Áreas	Treinamento
20/03/2025	00	Formatação Geral	SGI	SIM ( ) NÃO (X)

CÓPIA CONTROLADA