Bullbebtc
Descomplicada, inovadora e descentralizada

POLÍTICA
SEGURANÇA DA INFORMAÇÃO

A Proteção de Dados Pessoais, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. Além disso, é importante incluir as normas de boas práticas e as diretrizes de segurança cibernética, como a ISO 27001 e o NIST Cybersecurity Framework, para garantir a segurança das informações e prevenir ataques cibernéticos. Também é importante considerar a Política de Segurança Física, garantindo o acesso restrito e seguro às instalações onde os dados são armazenados e processados. A Política de Segurança da Informação deve ser atualizada regularmente para incluir novas leis, normas e diretrizes de segurança cibernética.

https://bullbebtc.com

Introdução

A segurança da informação é um conjunto de medidas e políticas que visam proteger informações confidenciais e sensíveis de uma organização. Isso inclui dados pessoais de clientes, informações financeiras, propriedade intelectual e outras informações importantes para a operação de uma empresa.

No mundo atual, onde a tecnologia se tornou uma ferramenta fundamental para empresas de todos os tamanhos e setores, a segurança da informação se tornou essencial. Isso é especialmente verdadeiro no Brasil, onde há muitos cibercriminosos agindo constantemente para invadir sistemas e roubar informações valiosas.

Quando as informações de uma empresa são expostas, ela pode enfrentar graves consequências, incluindo perda de reputação, multas e sanções governamentais, além de potencialmente prejudicar os clientes afetados pela violação de dados.

Portanto, garantir a segurança da informação é crucial para proteger o negócio e seus clientes contra ações maliciosas que podem colocar em risco informações confidenciais. É importante que as empresas implementem políticas de segurança da informação abrangentes e ofereçam treinamentos regulares para seus funcionários para manter os sistemas seguros e proteger os dados.

Objetivo

O presente documento tem como objetivo principal padronizar as diversas questões referentes à proteção de dados, de acordo com a Política de Segurança da Informação da empresa **BULLBEBTC.** Através da orientação e estabelecimento de diretrizes, a Política busca garantir a proteção dos ativos de informação da empresa, estabelecendo padrões comportamentais adequados às necessidades do negócio e garantindo a proteção legal da organização e de seus membros.

Somado a isso, a presente Política tem o objetivo de:

1. Assegurar que a **BULLBEBTC** irá atender à regulamentação vigente;

2. Fazer com que o nível de Segurança da empresa seja elevado e adequado;
3. Assegurar que todas as diretrizes postas nessa Política sejam colocadas em prática;

4. Impedir que softwares mal-intencionados invadam o sistema da empresa.

Aplicabilidade

As normas e recomendações contidas neste Política são aplicáveis a todos os colaboradores da **BULLBEBTC**, incluindo empregados, estagiários, aprendizes, Diretoria, membros do Conselho Superior e do Conselho Fiscal, prestadores de serviços e visitantes que tenham acesso às informações da empresa.

Todos os colaboradores da empresa têm o dever de observar e relatar quaisquer falhas, erros ou desvios em relação às práticas e procedimentos descritos neste documento. Essa é uma responsabilidade de todos, independentemente do cargo ou departamento. Esses relatórios devem ser feitos imediatamente, seja para o superior imediato ou para a Diretoria de Compliance, de acordo com a natureza e gravidade da inconsistência encontrada.

É importante ressaltar que o objetivo desses relatórios é garantir que as práticas e procedimentos de segurança da informação estejam sempre atualizados e em conformidade com as necessidades da empresa. Além disso, eles também servem como uma forma de prevenção e detecção de possíveis ameaças, permitindo que a empresa adote medidas preventivas e corretivas com rapidez e eficiência.

Revisão e Atualização

Este documento em particular foi produzido e deve ser interpretado em harmonia com os demais guias e Políticas vigentes na **BULLBEBTC**. Ele passará por revisões e atualizações anuais, ou em prazos menores, caso haja mudanças regulatórias ou legais, ou se a **BULLBEBTC** julgar necessário para incluir práticas relacionadas a atividades e procedimentos novos ou ainda não abordados. A responsabilidade por essa atualização é da Diretoria de Compliance, Controle Interno e Administrativo e de Tecnologia da Informação.

O que é a Segurança da Informação?

A proteção de informações é um tema contemporâneo e cada vez mais significativo, sobretudo no âmbito empresarial. É um tema de extrema importância e que merece uma atenção especial, visto que está em crescimento no Brasil e no mundo. Com a evolução tecnológica e o incessante fluxo de dados gerados a todo instante, aumenta também a necessidade de organizações estabelecerem Políticas e estratégias com o intuito de salvaguardar seus bens contra riscos e invasões cibernéticas que podem ocasionar perdas financeiras e danificar a imagem da empresa.

Pesquisas recentes apontam que apenas 17% das companhias estão completamente protegidas contra ameaças virtuais, tais como hackers e malwares. No Brasil, estatísticas do FortiGuard Labs revelam que somente no primeiro semestre de 2021, houve mais de 16

bilhões de tentativas de ataques virtuais. Diante desse cenário, é fundamental que as organizações se empenhem em adotar medidas preventivas e que possibilitem maior proteção para seus dados, bem como para os dados de seus clientes.

Dentro do ambiente empresarial, pode-se conceituar a segurança da informação como um conjunto de medidas e estratégias que têm por objetivo resguardar as informações produzidas e armazenadas em uma organização. Para que isso seja possível, práticas e políticas são adotadas para que possam garantir a conformidade da empresa, a fim de gerenciar os riscos e prevenir eventuais ameaças à confidencialidade, integridade, disponibilidade e autenticidade desses dados.

Essas atividades essenciais para a empresa são realizadas pelo setor de Compliance. Em outras palavras, o propósito da Segurança da Informação é proteger os dados corporativos contra acessos não autorizados, alterações indevidas, extravios, invasões aos sistemas e perdas de informações sensíveis e valiosas.

Como garantir a Segurança de Informações?

Desde o ano de 2018, o fluxo de informações no Brasil está sujeito às punições determinadas pela Lei Geral de Proteção de Dados (LGPD), a qual estabelece sanções severas para os infratores. Devido a isso, as empresas são obrigadas a criar mecanismos e investir em infraestrutura para evitar que os dados pessoais coletados em suas atividades sejam divulgados.

Esse é o caso, por exemplo, das informações bancárias, que são frequentemente alvo de ataques por parte de criminosos virtuais. Para isso, a segurança das informações nas empresas pode ser assegurada por meio de duas formas: **digitais e físicas**.

1. Digitais: Conhecidos também como controles virtuais, os controles lógicos são as medidas de segurança digitais utilizadas para restringir o acesso a informações sigilosas, como senhas, códigos e sistemas de proteção virtual. As principais formas de controle lógico são:

- **Assinatura eletrônica**: utilizada para autenticar documentos digitais;

- **Certificação digital**: uma espécie de selo eletrônico que comprova a autenticidade de um documento;

- **Hashing**: mecanismo de verificação que garante a integridade de arquivos;

- **Criptografia**: recurso utilizado para codificar o conteúdo de uma mensagem, a fim de dificultar a interceptação por terceiros;

- **Controles de acesso**: incluem senhas, logins, biometria, cartões de acesso, entre outros.

2. Físico: É importante ressaltar que a existência de monitoramentos lógicos não elimina a necessidade de implementar, também, os mecanismos de monitoramentos físicos, os quais pode-se citar:

- **Muros;**
- **Câmeras;**
- **Seguranças;**
- **Cofres;**
- **Fechaduras;**
- **Alarmes de segurança**
- **Portas.**

O que é considerado como ameaça para a Segurança da Informação?

A Segurança da Informação em uma empresa não é apenas uma questão de proteger contra os ataques cibernéticos, mas também de identificar e prevenir qualquer ameaça que possa comprometer a integridade, confidencialidade e disponibilidade dos dados. Ou seja, falhas humanas, como erros de configuração, descuidos com senhas e dispositivos perdidos, podem expor os dados a ameaças externas.

A proteção dos dados é uma responsabilidade compartilhada, que envolve não apenas a implementação de medidas preventivas e corretivas, mas também a conscientização e treinamento dos colaboradores para identificar e lidar com possíveis ameaças. Eventos naturais como incêndios, inundações e tempestades podem danificar equipamentos e infraestrutura, tornando os dados inacessíveis ou até mesmo perdidos, desse modo, se tornam, também, ameaças à Segurança da Informação.

O que são os “ativos” em Segurança da Informação?

De modo geral, pode-se dizer que **"ativo"** é tudo aquilo que é importante para a empresa e precisa ser protegido. São componentes como dados, equipamentos, softwares, usuários e

até mesmo as instalações físicas. Ou seja, podem ser relacionados aos espaços físicos, hardwares e softwares da empresa. Sem dúvidas alguma, esses ativos são de extrema importância para o negócio, seja do ponto de vista financeiro ou não, e por isso é fundamental garantir a segurança e a integridade dos mesmos.

A proteção dos ativos é feita através da implementação de Políticas e procedimentos que visam controlar os possíveis riscos e evitar que ameaças externas ou internas possam comprometer a segurança dos dados e informações da empresa. O objetivo em questão é minimizar os riscos e garantir a disponibilidade, confidencialidade e integridade dos ativos.

Os ativos podem ser classificados de diferentes formas, de acordo com sua importância, criticidade e grau de proteção. Devido a isso, é de grande necessidade que a empresa faça um inventário de todos os seus ativos, para saber quais são os mais críticos e quais precisam de mais proteção. Isso permite a criação de estratégias e ações específicas para garantir a segurança de cada um deles.

Responsabilidade da Área de Compliance

1. Auxiliar a **BULLBEBTC** na verificação de toda a legalidade das regulamentações e políticas utilizadas para proteger os ativos da empresa;

2. Em casos de violações de segurança, cabe ao Compliance liderar a apuração das causas e responsabilidades;

3. Assegurar que, de fato, as atividades realizadas dentro da empresa estarão de acordo com as políticas internas e regulamentações externas;

4. Diminuir o máximo possível os possíveis interesses de conflito dentro da empresa;

5. Aprovar a criação ou exclusão de usuários em caso de contratação ou demissão de colaboradores, garantindo que os usuários novos sejam cadastrados sem qualquer acesso e que o acesso seja concedido posteriormente pela gerência do colaborador;

6. Manter a política de perfis e acessos atualizada e solicitar à equipe de TI a liberação ou o bloqueio de perfis de acordo com as necessidades identificadas ou solicitadas pelos colaboradores.

É importante ressaltar que para garantir que as responsabilidades acima sejam cumpridas, a Diretoria de Compliance tem acesso irrestrito a todas as áreas da **BULLBEBTC**, incluindo salas com controle de acesso e toda a rede interna.

Responsabilidades da Gerência Jurídica

1. Certificar-se de que as diretrizes estabelecidas nesta política, assim como a necessidade de cumprimento de suas premissas, sejam mencionadas nos contratos e acordos com terceiros, assim como em contratos firmados com colaboradores da empresa. Isso irá garantir que todas as partes envolvidas estejam cientes de suas obrigações, direitos e deveres em relação a essa política.

2. Prestar suporte à Área de Compliance na criação e validação da conformidade legal de regulamentos, termos, políticas e controles utilizados para proteger os ativos de informação;

3. Assegurar que todos os contratos estabelecidos com terceiros contenham cláusulas de confidencialidade, preservando assim a segurança das informações da organização;

Responsabilidades dos Gestores das Áreas:

1. Identificar quaisquer violações às regras estabelecidas e tomar as medidas corretivas necessárias, informando imediatamente à Área de Compliance;

2. Fiscalizar o cumprimento desta Política por parte dos colaboradores e prestadores de serviços da empresa;

3. Informar à Diretoria de TI sobre quaisquer mudanças na equipe de colaboradores sob sua supervisão, como desligamentos, contratações ou transferências, para que os responsáveis possam atualizar as permissões de acesso correspondentes;

4. Impedir o acesso de ex-colaboradores ou funcionários demissionários aos ativos de informação da organização;

5. Proteger os ativos de informação e processamento da empresa contra ameaças internas e externas;

6. Assegurar que todos os funcionários sob sua liderança entendam e cumpram a obrigação de proteger os ativos de informação da empresa.

Responsabilidades da Diretoria de TI

1. Estipular as diretrizes de proteção dos recursos de informação da **BULLBEBTC**;

2. Remover ou desativar contas inativas;

3. Solicitar bloqueio de chaves de acesso de usuários, quando apropriado;

4. Revisar periodicamente as diretrizes estabelecidas para proteção;

5. Limitar e monitorar o acesso e privilégios de usuários externos e remotos;

6. Auxiliar as outras áreas da **BULLBEBTC** na elaboração e atualização do Plano de Continuidade de Negócios e de Contingência;

7. Identificar, registrar e reportar à gestão as tentativas de acesso não autorizado ou violações de segurança;

8. Definir e aplicar restrições de acesso à rede para cada usuário de TI, incluindo horários e dias autorizados.

9. Estabelecer prazo de validade para as contas de prestadores de serviço que corresponda ao período de contrato.

Gestão da Informação

Todas as informações produzidas ou recebidas pela **BULLBEBTC**, sejam elas em forma de dados, registros, arquivos ou documentos, são consideradas confidenciais por padrão, salvo quando há determinação legal ou regulatória para sua divulgação.

Cada colaborador é responsável por garantir a proteção adequada das informações confidenciais, e sempre que possível, indicar explicitamente a classificação de cada conjunto de informações, seja em fluxos de processo ou na própria documentação.

Todas as informações geradas ou acessadas pela **BULLBEBTC** e por terceiros são categorizadas em níveis de classificação, são eles:

1. Confidencial: Este é o nível mais elevado de segurança de informação estabelecido neste padrão. As informações classificadas como confidenciais são aquelas que, se divulgadas, têm potencial para causar danos financeiros significativos ou impactar negativamente a imagem da **BULLBEBTC**. Essas informações são protegidas por controles de acesso extremamente rigorosos e medidas de criptografia. Todos os colaboradores são obrigados a adotar medidas estritas para garantir a proteção e privacidade dessas informações confidenciais.

2. Restrita: Esse é um grau médio de segurança de informações confidenciais. Trata-se de informações que possuem um valor estratégico para a **BULLBEBTC** e que devem ser acessadas somente por um número limitado de colaboradores. Para garantir a sua proteção,

são utilizados controles de acesso a módulos específicos dos sistemas e/ou diretórios de armazenamento em nuvem.

3. Uso interno: Esse é o nível mais baixo de confidencialidade. As informações de uso interno são aquelas que não devem ser divulgadas para pessoas externas à organização, mas caso isso ocorra, não causarão grandes prejuízos financeiros ou danos à imagem da **BULLBEBTC**. A principal preocupação nesse nível está relacionada à integridade e à disponibilidade da informação, garantindo que as informações estejam atualizadas e acessíveis apenas para os colaboradores autorizados. São adotadas medidas de segurança para prevenir vazamentos acidentais ou intencionais, como controles de acesso e políticas de senhas seguras.

4. Pública: Esses dados não precisam de proteção mais avançada contra vazamentos, pois são de conhecimento público.

Gestão de Segurança Cibernética

O gerenciamento de acesso é uma prática fundamental para preservar a segurança das informações e evitar que indivíduos não autorizados acessem sistemas e ambientes que contêm dados confidenciais. Esse processo tem como objetivo principal garantir a confidencialidade das informações da organização, restringindo o acesso somente a usuários autorizados. Para assegurar um nível adequado de controle de acesso, são executados diversos processos.

Primeiramente, é necessário definir Políticas e Procedimentos de Segurança que estabeleçam as diretrizes para a concessão de acesso aos usuários, considerando as necessidades de cada função e departamento.

Em seguida, é preciso identificar e autenticar cada usuário que tenta acessar os sistemas e recursos. Isso pode ser feito por meio de senhas, tokens ou outros mecanismos de autenticação, que devem ser fortes o suficiente para evitar fraudes ou violações de segurança.

Além disso, é importante definir e gerenciar as permissões de acesso para cada usuário, restringindo o acesso apenas às informações e recursos que são necessários para o desempenho de suas funções. Também é necessário monitorar e auditar as atividades dos usuários, a fim de detectar possíveis anomalias e garantir a conformidade com as Políticas de Segurança estabelecidas.

Por fim, é importante revisar regularmente as políticas e procedimentos de segurança, para garantir que estejam alinhados com as necessidades da organização e com as melhores práticas de segurança da informação. Somente com um efetivo controle de acesso é possível garantir a confidencialidade das informações da organização e prevenir possíveis violações de segurança.

Para atingir um excelente nível de segurança, é necessário que a empresa atenda os seguintes requisitos:

1. Implementação de procedimentos formais para a concessão, alteração, revogação e gerenciamento de acessos, garantindo o princípio de menor privilégio e perfil mínimo restrito de acesso, em conformidade com a matriz de segregação de função;

2. Orientação aos usuários para que tenham acesso apenas às informações necessárias para a realização das atividades de negócio;

3. A equipe do gestor é responsável por informar os níveis de acesso aos novos colaboradores, com limitações de acesso aos ativos de informação sob o domínio da equipe do gestor;

4. A aprovação dos procedimentos de concessão e alteração de acesso dentro de uma equipe é realizada pelo gestor responsável e pela Diretoria de TI, garantindo o controle de acesso adequado e a segurança das informações.

Sigilo de Informações

Ao utilizar informações restritas ou confidenciais, os colaboradores da **BULLBEBTC** devem se atentar às seguintes questões:

1. É fundamental que os funcionários protejam a confidencialidade de todas as informações às quais tenham acesso durante o desempenho de suas funções na empresa. Essas informações não devem ser compartilhadas com terceiros, nem divulgadas e disponibilizadas ao público em geral. Além disso, não devem ser copiadas ou transferidas para dispositivos portáteis, como celulares, tablets ou computadores pessoais, nem enviadas para e-mails externos, mesmo que pertençam ao próprio funcionário.

2. O dever de manter sigilo mencionado anteriormente continua a ser obrigatório mesmo após o término do vínculo empregatício entre o colaborador e a **BULLBEBTC**, independentemente do motivo da rescisão. Portanto, o colaborador permanece obrigado a manter a confidencialidade e a proteger as informações obtidas durante o período em que trabalhou na empresa.

3. Cada colaborador é individualmente responsável, tanto na esfera civil quanto criminal, pela divulgação indevida de informações confidenciais ou qualquer outra informação que tenha como objetivo difamar a imagem da empresa ou prejudicar seu relacionamento com clientes. A divulgação não autorizada de informações confidenciais pode gerar consequências graves para a empresa, como perda de vantagem competitiva, prejuízos financeiros e danos

à sua imagem no mercado. Por essa razão, é importante que os colaboradores compreendam a seriedade dessa questão e a responsabilidade que possuem em relação a ela.

4. Para proteger a segurança e confidencialidade das informações restritas e confidenciais da empresa, é essencial que os colaboradores evitem discutir esses assuntos em locais públicos, como corredores, elevadores, meios de transporte coletivos, restaurantes, entre outros.

5. Os programas de e-mail disponibilizados pela **BULLBEBTC** devem ser usados exclusivamente para comunicações profissionais. Não é permitido sob hipótese alguma o uso dessas ferramentas para enviar ou encaminhar mensagens ou seus anexos que possam prejudicar a imagem da empresa.

6. As informações confidenciais dos clientes que são recebidas ou fornecidas à **BULLBEBTC** para a execução de transações estão protegidas por legislação específica. Esses dados não podem ser compartilhados com terceiros sem uma autorização expressa e por escrito dos próprios clientes.

Sobre a Privacidade

As comunicações internas, tais como ligações telefônicas, e-mails e outros canais, são monitoradas e armazenadas pela **BULLBEBTC,** que tem o direito de consultar esses registros sem aviso prévio ao colaborador. No entanto, a privacidade do colaborador é respeitada, desde que ele utilize os recursos da empresa para fins profissionais e não viole a Políticas de Segurança da Informação da **BULLBEBTC**.

Vale ressaltar que a empresa tem o dever de proteger as informações confidenciais e restritas, que são propriedade da **BULLBEBTC** e seus clientes, e o monitoramento é uma medida de segurança para garantir a integridade dessas informações. O colaborador deve estar ciente dessas políticas e responsabilidades, evitando o uso indevido dos recursos da empresa e contribuindo para um ambiente seguro e confiável.

Controle Contra Software Malicioso

Para garantir a segurança dos dados armazenados nos equipamentos da **BULLBEBTC**, é essencial que todos os computadores tenham um software antivírus instalado e atualizado diariamente de forma automática. Malwares de computador podem causar perda ou alteração de dados, o que pode ser prejudicial para a empresa. Caso o colaborador receba alertas de vírus provenientes de fontes diferentes do antivírus da **BULLBEBTC**, é importante que ele não os acesse nem os encaminhe para outras pessoas.

Em muitos casos, esses alertas são falsos e podem levar a comprometimento da segurança do sistema. Se houver dúvida, é recomendável entrar em contato com a área de Tecnologia da **BULLBEBTC** para obter suporte técnico.

Casos de Incidentes à Segurança da Informação

As respostas aos incidentes de Segurança da Informação são desenvolvidas com o objetivo de garantir o retorno ao nível normal do ambiente tecnológico, após o ocorrido de um caso atípico. Para isso, são utilizados recursos e procedimentos fundamentais que visam garantir uma resposta efetiva, minimizando os danos causados.

As equipes responsáveis pela Segurança da Informação da **BULLBEBTC** são treinadas para lidar com os incidentes de forma ágil e eficiente. São utilizados procedimentos padrão, que envolvem a análise das causas do incidente, a identificação dos danos e a aplicação de medidas corretivas e preventivas.

É importante ressaltar que a **BULLBEBTC** investe constantemente em medidas de prevenção e proteção, a fim de minimizar a ocorrência de incidentes de Segurança da Informação. No entanto, caso aconteça algum incidente, a empresa está preparada para agir de forma rápida e eficiente, garantindo a segurança dos dados e a continuidade dos negócios.

Procedimentos

Políticas de senha fortes devem ser implementadas para todos os usuários. As senhas devem ser alteradas regularmente e nunca compartilhadas.

Os empregados devem ser treinados sobre como lidar com informações confidenciais e pessoais e devem assinar um acordo de confidencialidade;

A política de acesso às informações deve ser estabelecida para todos os usuários. Os acessos devem ser limitados somente àqueles usuários que precisam das informações para desempenhar suas funções e, quando necessário, concedidos mediante permissão formal;

Os computadores devem ter softwares antivírus e anti-spyware para minimizar os riscos de malwares;
Backups regulares de dados devem ser feitos e mantidos fora do local para minimizar o risco de perda de informações.

Revisão

A política de segurança da informação deve ser revisada anualmente ou sempre que ocorrerem mudanças importantes na organização ou no ambiente.

Conclusão

Esta Política de Segurança da Informação abrange as principais diretrizes e procedimentos a serem seguidos na proteção das informações da organização. A implementação rigorosa desta política ajudará a reduzir os riscos de perda ou comprometimento das informações críticas da organização.

A falta de conhecimento em relação às obrigações e compromissos estabelecidos neste documento não justifica eventuais desvios. Em caso de dúvidas ou necessidade de esclarecimentos adicionais, é recomendado consultar a área responsável pelo Compliance na empresa. O não cumprimento das normas aqui estabelecidas pode resultar em medidas disciplinares, administrativas ou judiciais, incluindo a possibilidade de demissão e outras sanções previstas em leis, regulamentos e normas aplicáveis.

Esta política de Segurança da Informação é de propriedade exclusiva da **BULLBEBTC** e é protegida por lei contra a sua reprodução, distribuição, cópia ou uso não autorizado. Qualquer violação desses direitos pode resultar em medidas legais apropriadas.

É importante ressaltar que esta política de Segurança da Informação foi elaborada especificamente para as necessidades da **BULLBEBTC** e não deve ser copiada ou usada por outras empresas sem autorização expressa da nossa organização.

DATA	COMPLIANCE	DIRETOR
15/05/2023	DocuSigned by: Vera Cavalcanti FB887C6A4CF04D0...	DocuSigned by: Paulo Ricardo Oliveira Braga 89EA2F82CEA14D7...