POLÍTICA DE SEGURANÇA E CONTROLE DA INFORMAÇÃO – PSCI

A Política de Segurança e Controle da Informação também referido como PSCI é o documento que orienta e estabelece normas e condutas, na Bitcoin To You, para o controle e proteção das informações e a responsabilidade legal para todos os usuários dessa, se fazendo presente de forma orgânica na cultura da organização.

I – REFERÊNCIA DA PSCI

A presente PSCI está baseada nas recomendações e objetivos de controle elencados pela norma ABNT NBR ISSO/IEC 27002/2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, assim como está de acordo com as publicações NIST e seu Framework de Segurança da Informação e as normas legais vigentes no país.

II – RELEVÂNCIA DA PSCI

Os sistemas de informação da Bitcoin To You bem como sua rede de dados sofrem diversos tipos de ameaças à segurança da informação, como cibercriminosos, malwares, hackers e diversos tipos de ataques de negação de serviço estão se tornando cada vez mais frequentes e incrivelmente sofisticados. Tal realidade que se estende não só a Bitcoin To You, mas para as exchanges de forma geral, é critica, e devido a isso a relevância em se ter uma PSCI bem fundamentada e enraizada na cultura organizacional.

Entende-se que não basta apenas ter uma PSCI, ter ela bem fundamentada na cultura da empresa, ela deve ser aplicada diariamente e controlada, pois os riscos a segurança vão se modificando e junto a eles a Bitcoin To You se modifica também, dando mais relevância e importância a segurança de suas operações.

III – OBJETIVOS

O objetivo da PSCI é estabelecer diretrizes que possibilitem os clientes, fornecedores e colaboradores da Bitcoin To You seguirem padrões de comportamento que assegurem a manutenção do controle e segurança quanto a informação usualmente utilizada e processada no negócio.

Para atingir tal objetivo é necessário que tais comportamentos se atentem a normas e procedimentos específicos de segurança da informação e condizentes com os controles para a manutenção e gestão da informação. Nesse sentido o objetivo geral se desmembra os seguintes objetivos específicos.

- Integridade: a informação deve preservar seu estado original, ser íntegra e protegida quanto a alterações indevidas, intencionais ou acidentais. Os controles e processos devem garantir a integridade do próprio design dos produtos e sistemas da Bitcoin To You.
- Confidencialidade: não é permitido nenhuma contratação de colaboradores sem assinatura de Termo de Sigilo e Confidencialidade, além disso, é vedado qualquer disponibilização de informações dos clientes, contratos, processos e outros a terceiros, salvo por exigência legal. As demais informações dos clientes, são acessadas apenas por eles próprios.
- Disponibilidade: é garantido aos usuários o acesso as informações que sejam pertinentes a eles próprios, garantindo também a confidencialidade e integridade do conteúdo disponibilizado.

IV – APLICAÇÃO DA PSCI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores (independentemente do nível hierárquico ocupado), clientes e prestadores de serviço da Bitcoin To You, e se aplicam à informação em qualquer meio ou suporte.

É obrigação de cada colaborador se manter atualizado quanto as normas, aplicação e atualização da PSCI bem como aos procedimentos relacionados, buscando orientação ao manutentor da PSCI sempre que houver dúvidas, ou na hipótese em que estiver em dúvidas, ao estar frente a situação de aquisição, uso e/ou descarte de informações.

V – PRINCÍPIOS DA PSCI

Os princípios norteadores da PSCI são:

- Princípio da Produção e Propriedade da Informação: A Bitcoin To You exerce atividade com grande volume de produção de informação. Esse princípio leva em consideração que toda informação produzidas em decorrência da atividade profissional da empresa pertencem a mesma, salvo exceções, formalizadas entre as partes relacionadas.
- Princípio da Utilização de Recursos: Todos os equipamentos que trafegam informações, como equipamentos de informática, comunicação, sistemas, sofwares entre outros, podem ser utilizados pelos colaboradores desde que estes utilizem de forma íntegra, confidencial e segura, de acordo com os objetivos previstos na PSCI.
- Princípio da Segurança da Informação: A Bitcoin To You no exercício da PSCI poderá registrar os acessos, descartes, inclusões, aquisições, variações e utilização de informações, visando garantir a disponibilidade e segurança da informação de acordo com os objetivos previstos na PSCI.

VI – REQUISITOS DA PSCI

São requisitos para a Política de Segurança e Controle da Informação os elencados abaixo:

- A referida Política deverá ser comunicada e disponibilizada a todos os colaboradores da Bitcoin To You de forma que a mesma seja cumprida dentro e fora da organização;

- Será constituído um comitê multidisciplinar responsável pela gestão e controle da segurança da informação, denominado de COMITÊ DE SEGURANÇA DA INFORMAÇÃO;
- A PSCI deverá ser atualizada e revista periodicamente ou sempre que um fato superveniente ocorrer, motivando a revisão antecipada;
- Todos os contratos praticados pela Bitcoin To You deverão vir precedidos de Cláusula de Confidencialidade ou Acordo de Confidencialidade;
- Todos os colaboradores no momento da admissão deverão ser comunicados sobre o PSCI e também deverão assinar o Termo de Sigilo e Confidencialidade. Além da assinatura eles deverão ser instruídos sobre os procedimentos de segurança, bem como o manuseio correto dos equipamentos de informativa, sistemas, softwares, meios de comunicação e outros, com objetivo de reduzir possíveis riscos a proteção da informação;
- Em situações de incidentes que afetem a segurança da informação, esses deverão ser comunicados ao manutentor do PSCI e encaminhados ao Comitê de Segurança da Informação para análise;
- Deverão ser criadas ferramentas de controle e gestão da segurança da informação;
- Deverá ser implantado plano de ação para monitoramento dos equipamentos informatizados, meios de comunicação, sistemas e outros com objetivo de agir previamente em situações de possíveis riscos a informação;
- O não cumprimento dos requisitos previstos na PSCI acarretará violação às normas internas da Bitcoin to You podendo ocasionar medidas administrativas e legais cabíveis.

VII – ORGANIZAÇÃO E RESPONSABILIDADES ESPECÍFICAS DA PSCI

- Diretores

Ter postura exemplar em relação a segurança da informação, apoiando ativamente a cultura de segurança da informação como valor estratégico da Bitcoin To You.

Definir estratégias de Segurança da Informação, alinhando a mesma às demais estratégias do negócio.

Exigir dos colaboradores a assinatura do Termo de Sigilo e Confidencialidade e cumprimento das diretrizes e normas previstas na PSCI.

Deliberar sobre a criação e regulamentação do Comitê de Segurança da Informação.

Realizar periodicamente e/ou sempre que necessárias reuniões junto ao Comitê de Segurança da Informação.

Assinar e aprovar documentos que estejam de acordo com as diretrizes do PSCI.

- Colaboradores

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

Os colaboradores devem ser responsáveis e devem ser organizar para conhecer e cumprir rigorosamente a referida PSCI.

Devem ter ciência que todo dano ou prejuízo que vier a sofrer ou causar a Bitcoin To You e/ou a terceiros em decorrência da não obediência às diretrizes e normas estabelecidas pela PSCI.

Devem se atentar e reportar ao se deparar com práticas em não conformidade com a PSCI, ajudando, inclusive, na reeducação dos hábitos em não conformidade.

Reportar ao Comitê de Segurança da Informação a suspeita ou indicio de violação das normas e diretrizes previstas nesse instrumento, falhas em controles de segurança da informação, tentativas de quebra de sigilo ou confidencialidade da informação, ou qualquer outra atividade que vá em desacordo com a aplicação da preferida PSCI.

- Comitê de Segurança da Informação

O Comitê de Segurança da Informação deve ser formalmente constituído por profissionais de nível hierárquico mínimo gerencial, nomeados para participar do grupo pelo período de um ano.

Deve criar procedimentos e políticas que garantam o controle e segurança da informação na Bitcoin To You. Deve analisar as situações de inconformidades e riscos a segurança da informação.

Deve monitorar a execução do plano de ação de monitoramento preventivo da segurança da informação e reunir-se formalmente pelo menos uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário.

Revisar o PSCI sempre que necessário e providenciar treinamento e atualização dos colaboradores e partes envolvidas. Se necessário poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

Deve providenciar treinamento aos colaboradores e partes envolvidas em períodos de 24 a 24 meses de forma a garantir reciclagem dos mesmos objetivando maios eficiência no controle e segurança da informação.

Revisar e controlar os procedimentos para recuperação de falhas, desastres e resposta a incidentes que afetem a disponibilidade dos Sistemas de Informação da Bitcoin To You.

Articular e fomentar à cultura de controle, proteção e segurança da informação dentro da Bitcoin To You e em toda a cadeia de relacionamentos da empresa.

Gerenciar a realização de testes de vulnerabilidades periódicos, abrangendo a rede internet e intranet da empresa, a fim de identificar as ameaças existentes e aplicar as devidas correções para qualquer vulnerabilidade exposta.

VIII – GESTÃO E CONTROLE DA INFORMAÇÃO

- Área de Tecnologia da Informação

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

Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSCI.

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Garantir segurança especial para sistemas com acesso público como o software de gestão, compra e venda de criptoativos, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Bitcoin To You. Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

a) os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário;
b) os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a

auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da empresa.

Realizar auditorias periódicas de configurações técnicas e análise de riscos.

Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

Monitorar o ambiente de TI, gerando indicadores e históricos de:

a) uso da capacidade instalada da rede e dos equipamentos;
b) tempo de resposta no acesso à internet e aos sistemas críticos da Bitcoin To You;
c) períodos de indisponibilidade no acesso à internet e aos sistemas críticos da Bitcoin To You;
d) incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
e) atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

- Área de Segurança da Informação

Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.

Propor e apoiar iniciativas que visem à segurança dos ativos de informação da Bitcoin To You. Publicar e promover as versões da PSCI e as Normas de Segurança da Informação aprovadas pelo Comitê de Segurança da Informação.

Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da Bitcoin To You, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação.

Apresentar as atas e os resumos das reuniões do Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do próprio comitê ou de outros membros da diretoria.

Manter comunicação efetiva com o Comitê de Segurança da Informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a Bitcoin To You.

Buscar alinhamento com as diretrizes corporativas da instituição.

XIX – MONITORAMENTO E AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta PSCI a Bitcoin To You poderá:

- implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação;
- realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

ARMAZENAMENTO E TRANSMISSÃO DE INFORMAÇÕES CONFIDENCIAIS

Atendendo aos requisitos contratuais de sigilo, os meios de armazenamento previamente aprovados são: discos criptografados, transmissão por rede ou internet utilizando SSL (com certificado de origem e destino da transmissão pertencentes às partes acordadas em contrato), SSH ou SFTP (FTP via SSH). Para transmissão de informações confidenciais por e-mail em servidores e domínios diferentes, é necessário adicionar criptografia adicional em nível de arquivo (senha no arquivo utilizando criptografia forte de no mínimo AES 1024 bits ou equivalente). A proteção por senha deve ser aplicada INCLUSIVE para proteção de certificados privados de uso geral (por exemplo, ao se gerar pares de chaves SSH, é necessário aplicar senha FORTE nas chaves privadas).

Deverão ser classificadas como confidenciais as informações que por sua origem, natureza ou importância não devam ser compartilhadas ou colocadas à disposição de pessoas não autorizadas. Consideram-se Informações confidenciais todas as que assim forem classificadas, bem como – indistintamente – dados recebidos ou compilados de/sobre clientes, senhas, informações financeiras ou de salários, código fonte, informações sensíveis de usuários entre outras.

SECRETAS: as informações classificadas como SECRETAS possuem o mais alto nível de sensibilidade e criticidade para o negócio. Carteiras de bitcoin em geral, chaves de criptografia (certificados SSL ou chaves SSH) e credenciais de acesso em geral são exemplos de informações SECRETAS. Outras informações estratégicas com alto nível de confidencialidade também podem ser classificadas como SECRETAS a critério do proprietário da informação.

Informações em que seu possível vazamento implica em impacto financeiro direto ao negócio ou ponha em risco a continuidade dos negócios é um indício para que ela receba a classificação máxima de proteção: SECRETA.

As informações secretas normalmente possuem os seguintes controles e proteções:

a) São armazenadas em volumes criptográficos acrescidos de criptografia de arquivo: criptografia multinível com chaves e algoritmos distintos.
b) O acesso à informação SECRETA é feito sempre que possível em equipamento OFF-LINE, em ambiente controlado sem que outros atores não estejam no recinto.
c) As informações SECRETAS não podem ser copiadas, fotografadas, filmadas (incluindo sistemas de CFTV) ou testemunhadas, pessoalmente ou por meio de telepresença de qualquer forma.
d) Algumas informações secretas podem simplesmente não serem armazenadas (brain storage only), processadas ou transmitidas no ambiente computacional da Bitcoin To You sempre que isso for possível.
e) Carteiras de criptomoedas de fluxo de transações (hot wallets): só poderão ser armazenadas em servidores de produção utilizando-se de criptografia forte adicionalmente à criptografia de disco, só devendo ser lida em seu formato aberto em memória do mesmo servidor e de forma temporária ao tempo das transações estritamente necessárias as movimentações do Bitcoin To You e seus clientes.

f) Carteiras de criptomoedas de reserva ou custódia (cold wallets): O armazenamento é offline, o acesso é via dispositivo offline.

A classificação dos documentos deverá ocorrer em campo visível, preferencialmente na primeira página e próximo ao cabeçalho do Documento.

Quando um Documento contiver mais de um tipo de informação com classificação original distintas, por exemplo, dois documentos unidos em um único arquivo, a classificação mais restritiva passa a valer para todo o documento.

Qualquer informação que não tenha sua classificação especificadade forma clara no documento será automaticamente considerada como informação “RESTRITA”.

ATRIBUIÇÃO INICIAL DA CLASSIFICAÇÃO À INFORMAÇÃO

Caberá ao colaborador AUTOR da informação definir os acessos, níveis de permissão e formas de proteção quando se tratar de uma informação RESTRITA, CONFIDENCIAL ou SECRETA.

Será considerado como AUTOR da informação o colaborador que primeiro produzir ou manipular a informação dentro do ambiente da Bitcoin To You.

Todo colaborador será responsável pela sua classificação e armazenamento, seguindo as recomendações contidas neste documento.

Caberá à área de segurança da informação, prover o suporte técnico aos autores das informações geradas e realizar os devidos treinamentos sobre proteção e armazenamento seguro de dados.

A área de Tecnologia da Informação é a provedora dos recursos e meios de armazenamentos seguro dessas informações, assim como as ferramentas de controle de acesso, proteção e criptografia.

PUBLICAÇÃO DE INFORMAÇÕES ABERTAS

Somente os gestores da Bitcoin To You, com assessoria devida das áreas de Comunicação e Marketing, poderão classificar informações para divulgar externamente ou as definir como Informação Pública.

DO USO DAS FERRAMENTAS CORPORATIVAS

A Bitcoin To You poderá fornecer ao colaborador contas de correio eletrônico, acesso à internet e outras ferramentas de comunicação e produtividade para a dinamização do trabalho ou utensílios como gavetas, armários e quaisquer dispositivo físico ou lógico para a execução do trabalho.

O uso destas ferramentas estará sujeito a esta política de segurança da informação e restrições de acesso, de acordo com o nível de acesso outorgado ao usuário e deliberações do Comitê de Segurança da Informação.
Como política de nível de acesso à informação, utilizamos a premissa de “menor privilégio possível”. O colaborador somente terá acesso aos aplicativos e informações que forem estritamente necessários para a realização do seu trabalho.

É expressamente proibido o uso de qualquer recurso corporativo, computadores, redes, acessos bem como quaisquer meios de comunicação corporativas para a prática de qualquer ato ilícito sob pena de responsabilidades civis ou até criminais.

ACESSO E USO DA INTERNET

A Bitcoin To You poderá permitir a navegação em sites de conteúdo e acesso à Internet, sempre de acordo com a sua política de segurança da informação e bloqueios de sites classificados como inseguros ou não confiáveis.

É explicitamente proibido a transferência de arquivos por meio de quaisquer protocolo, aplicativo ou ferramenta que não forem previamente e explicitamente aprovados pela área se segurança da Informação da Bitcoin To You.

Essa aprovação é, na verdade, uma análise de segurança da ferramenta e do fornecedor do produto, a fim de garantirmos que somente ferramentas e fabricantes que possuam alta maturidade em segurança da informação, proteção de dados e políticas claras de privacidade sejam incorporados à lista de ferramentas e fornecedores aprovados.

Isso evita a herança de vulnerabilidades por meio de ferramentas não seguras e não testadas, assim como parcerias com fornecedores que possam não seguir as boas práticas de segurança da informação.

Da mesma forma, não será permitido o download de materiais protegidos por direitos autorais ou a instalação de softwares não homologados pela área de Segurança da Informação.

E-MAIL / CORREIO ELETRÔNICO

O correio eletrônico da Bitcoin To You, assim como todas as plataformas de comunicação utilizadas na empresa, são ferramentas de trabalho, não devendo ser utilizado para outros fins.

As informações contidas nas mensagens eletrônicas são de propriedade da Bitcoin To You podendo ser monitoradas a qualquer tempo sem aviso ou notificação prévia para fins de auditoria de conformidade às normas internas, regulamentações ou boas práticas aplicadas ao negócio da Bitcoin To You.

É expressamente proibido o envio de informações classificadas como “INTERNAS” e “CONFIDENCIAIS” para endereços de e-mail fora do domínio bitcointoyou.com exceto para terceiros (clientes ou fornecedores) diretamente envolvidos no assunto em questão.

As informações classificadas como SECRETAS não devem ser armazenadas ou transmitidas por e-mail simples. Para isso, é mandatório o uso de criptografia forte adicional para proteção do conteúdo da mensagem e seus anexos.

SENHAS DE ACESSO

A senha de acesso aos recursos computacionais da Bitcoin To You é de inteira responsabilidade do colaborador que não deverá, em hipótese alguma, compartilhar ou emprestar a outros colaboradores e terceiros.

Os usuários deverão utilizar senhas “fortes”, misturando letras e números, em todos os sistemas corporativos e o tamanho mínimo recomendado para as senhas é de 8 (oito) caracteres.

Informações classificadas como SECRETAS deverão obrigatoriamente utilizar uma sequência longa de pelo menos 18 caracteres, ou optar pela utilização de uma chave específica de pelo menos 1024 bits (utilizando-se sempre uma senha adicional para a proteção da chave criptográfica).

Toda ação feita, dentro ou fora do ambiente computacional da Bitcoin To You, será de responsabilidade do colaborador associado às credenciais de acesso associadas às ações.

CONTAS INATIVAS

Toda e qualquer credencial de acesso que não tiver atividade em até 90 dias serão bloqueadas em TODOS os sistemas corporativos.

AUTENTICAÇÃO DE MULTI FATOR (DOIS FATORES)

É obrigatório o uso de autenticação multi-fator (2FA ou MFA; Two factor Authentication ou Multi-Factor Authentication) para TODOS os serviços onde a opção estiver disponível.

ACESSO REMOTO

Colaboradores previamente cadastrados, mediante aprovação explícita dos seus gestores diretos, poderão obter acesso remoto ao ambiente computacional da Bitcoin To You. Para isso, é necessário o preenchimento do formulário que indica a vigência inicial e final do acesso, sua necessidade e níveis de acesso externo. Esse processo deve usar equipamentos corporativos fornecidos pela Bitcoin To You com a aplicação dos controles de segurança vigentes. A conexão será estabelecida por meio de VPN privada corporativa.

DOCUMENTOS NA MESA

Todos os colaboradores deverão obedecer as regras de limpeza e organização do ambiente de trabalho a fim de não expor desnecessariamente informações classificadas.

Os documentos impressos e anotações que precisem estar em um papel (impresso ou anotações) devem permanecer nas mesas em caráter temporário devendo ser recolhidos em compartimentos fechados disponíveis em seu departamento ou qualquer dependência da empresa que forneça segurança e proteção a esses materiais.

Toda informação que permanecer nas mesas poderá e deverá ser destruída pelo colaborador responsável ou por qualquer outro colaborador que assim o quiser fazê-lo exercitando as boas práticas de proteção de informações da Bitcoin To You.

Os documentos órfãos notoriamente importantes (que possuem assinaturas por exemplo) deverão ser depositados em um armário especial do tipo boca de lobo para que possam ser revisados posteriormente antes de sua destruição - cofre de documentos órfãos localizados ao lado das impressoras.

Esta regra vale para o ambiente de trabalho, incluindo a estação de trabalho, mesa, gavetas, arquivos e lixo.

BLOQUEIO DE DISPOSITIVOS POR INATIVIDADDE

Todo dispositivo corporativo de acesso aos sistemas corporativos devem sofrer bloqueio automático depois de 10 minutos de inatividade (computadores, smartphones, tablets ou qualquer outro dispositivo, móvel ou não).

CAPTURA DE TRÁFEGO NA REDE

É expressamente proibido a captura de tráfego de rede dentro da rede corporativa da Bitcoin To You salvo eventos devidamente autorizados pelo Comitê de Segurança ou pelo gestor de segurança para fins exclusivos de diagnóstico, auditoria e monitoração previamente autorizados.

DISPOSITIVOS PESSOAIS

O uso de dispositivos pessoais fica restrito a rede de convidados/guest da Bitcoin To You.

Não é permitido a conexão de dispositivos não corporativos as redes internas, cabeadas ou sem fio.

Aos colaboradores que precisem fazer uso de dispositivos móveis para o desempenho de funções e tarefas específicas, o farão utilizando equipamentos fornecidos pela empresa, com os devidos controles e proteções técnicas aplicadas.

REDES SOCIAIS

É expressamente proibido que qualquer colaborador emita qualquer comunicado, opinião ou comentário em nome da Bitcoin To You sem a expressão aprovação e alinhamento com a área de marketing e comunicação.

As interações de resposta, réplica aos comentários feitos por terceiros sobre a empresa e afins, só podem ser feitas pelas áreas específicas de comunicação e gestão de mídias sociais.

A publicação de fotos em área internas também devem ser evitadas, para evitar que informações restritas contidas nas áreas internas da empresa sejam publicadas inadvertidamente.

SOFTWARE, APPS E PLUGINS

Não é permitido a instalação de softwares não aprovados pela área de TI e Segurança em quaisquer dispositivos que acessam os sistemas de informação da Bitcoin To You que inclui: computadores, notebooks e dispositivos portáteis como tablets e celulares. Inclusive software, aplicativos, plugins pagos ou gratuitos.

A área de TI e Segurança já possui um portfólio de ferramentas e aplicativos para atender as demandas do negócio incluindo ferramentas de produtividade e afins.

A maioria dessas ferramentas já são previamente instaladas em todos os dispositivos corporativos.

POSTURA GERAL DE PRIVACIDADE

Todos os acessos aos sistemas internos devem ter como justificativa um propósito real de negócio.

É expressamente proibido o acesso a quaisquer informações de clientes, colaboradores ou qualquer registro nos sistemas de informação da Bitcoin To You sem um propósito claro de negócio, e ligado diretamente ao exercício das funções atribuídas na relação de trabalho entre o colaborador e a empresa.

É expressamente proibido o acesso a dados de clientes por mera curiosidade.

Como por exemplo:

Acessar contas de celebridades, pessoas públicas, parentes, amigos ou qualquer outro cliente sem que haja um propósito de negócio e principalmente, um chamado relacionado ao caso. Caso precise resolver algum problema na sua própria conta, como por exemplo aprovar um depósito, abra um chamado e peça que um colega faça a aprovação para você.

MONITORAÇÃO

A Bitcoin To You se reserva ao direito de monitorar todas as atividades feitas pelos seus colaboradores em seus sistemas de informação para garantir o cumprimento desta e outras políticas da empresa.

Os ambientes internos da Bitcoin To You também podem sofrer gravação audiovisual com o propósito principal de aumentar a segurança do perímetro interno da empresa contra incidentes de segurança de qualquer natureza.

ACESSO AO ESCRITÓRIO E ESCOLTA DE VISITANTES

O acesso ao nossos escritórios NÃO pode ser feito por pessoas DESACOMPANHADAS. Um colaborador sempre deverá escoltar o visitante DESDE a chegada na recepção do prédio, até a entrada no escritório.

A recepção NÃO deve abrir a porta de acesso, ou seja, quem não possui biometria cadastrada, sempre terá que ser escoltado por outro colaborador. Para colaboradores ou consultores externos que trabalhem mais de dois dias por semana no escritório, iremos cadastrar sua biometria e liberar o acesso sem escolta.

A porta principal DEVE PERMANECER SEMPRE FECHADA, mesmo para saídas rápidas do escritório (colocar detritos e lixos no compartimento do andar, por exemplo). Antes de abrir a porta, sempre OBSERVE com cuidado QUEM

está no hall dos elevadores, na parte externa do escritório. Se houver presença de estranhos NÃO abram a porta, retornem a recepção e aguarde alguns minutos antes de retornar ao andar. Se necessário peça a segurança do prédio para subir ao andar, verificar e escoltar a pessoa para o andar correto (ele pode simplesmente ser de outra empresa e ter descido no andar errado ;)

Os pontos chaves desse capítulo são:

- A recepção INTERNA não deve abrir a porta para dar acesso ao escritório;
- Todos os visitantes devem ser escoltados DESDE a recepção do prédio;
- Não autorizamos que visitantes SUBAM ao nosso andar sem escolta de um colaborador;
- Não atendemos clientes do Bitcoin To You em nosso escritório;
- Só abra a porta depois de verificar se estranhos não estão no andar

GRAVAÇÃO DE CONTEÚDO AUDIOVISUAL NAS DEPENDÊNCIAS DA EMPRESA

Eventualmente as áreas de negócios, lideradas pelo marketing poderão fazer gravações de áudio e vídeo dentro das dependências da empresa. Esta sessão trás algumas recomendações e obrigação a serem observadas durante esses eventos:

a) Os profissionais que farão a captação do conteúdo, quando não forem colaboradores diretos da empresa deverão estar sob supervisão direta durante toda a permanência na empresa de pelo menos um colaborador;
b) A empresa contratada, assim como quaisquer fornecedores, devem ter um NDA assinado e vigente ANTES da realização dos trabalhos;
c) O colaborador e área cliente do trabalho, será o responsável pela observância de qualquer informação confidencial como telas, documentos, anotações (inclusive nos quadros localizados nas paredes usados para notas pelas equipes) garantindo que essas informações não sejam capturadas pelas fotos ou vídeos realizados

dentro de nossas dependências. O fornecedor ainda, deve revisar e ofuscar qualquer conteúdo que for observado durante a edição do material e a área contratante deve sempre revisar a versão final da produção audiovisual para assegurar que informações confidenciais não tenham acidentalmente sido capturadas nas imagens.

X - DAS DISPOSIÇÕES FINAIS

A violação desta política poderá acarretar em sanções administrativas e/ou legais, inclusive com rescisão do contrato de trabalho e/ou qualquer outro contrato de relacionamento de prestação de serviço entre o colaborador, associado, consultor e/ou sócio, assim como qualquer entidade com relação contratual direta ou indireta com a Bitcoin To You.