INDIGO INVESTIMENTOS

Política de Segurança Cibernética

2022

Sumário

1. OBJETIVO

A Política de Segurança da Informação visa preservar a confidencialidade, integridade e disponibilidade das informações utilizadas pela INDIGO DTVM no desempenho de suas atividades, descrevendo a conduta adequada para o seu manuseio, controle, proteção e descarte, bem como estabelecer regras para acesso físico às instalações da INDIGO DTVM.

Tem como diretrizes básicas os seguintes aspectos:

- Garantir que toda informação tenha a proteção necessária no seu manuseio, tratamento e divulgação, determinando limites de comportamento e medidas a serem tomadas no caso de sua violação em consonância com o presente documento;
- Definir diretrizes e responsabilidades que devem subsidiar a elaboração de normas, procedimentos e padrões de proteção da informação, abrangendo sua geração, utilização, armazenamento e distribuição;
- Garantir a disponibilidade, integridade e confidencialidade da informação, independente do meio de armazenamento;
- Garantir a segurança e proteção das informações na prática de trabalho em home-office.
- Garantir que a informação seja utilizada por quem necessita para a execução de suas atividades diárias;
- Evitar que usuários possam fazer o uso da informação de forma mal-intencionada, para obtenção de benefícios próprios;
- Estabelecer subsídios para as implementações de cláusulas específicas nos contratos que visam garantir que a informação tenha a devida proteção;

2. REGULAMENTAÇÃO APLICÁVEL

- Resolução Bacen 4.658/2018;
- Lei 9.609/98 – Lei do Software;
- Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros.

3. VIGÊNCIA

As diretrizes contidas neste documento entram em vigor na data de sua publicação e permanecem vigentes por prazo indeterminado, devendo ser revisado anualmente.

A aprovação deste manual e posterior atualizações deverão ser realizadas por todos os Diretores da INDIGO DTVM, com a aprovação registrada em ata assinada pelos mesmos.

4. PÚBLICO-ALVO

Essa política tem como público-alvo todos os funcionários da INDIGO DTVM, bem como todo e qualquer colaborador que presta serviços em seu nome.

A Política de Segurança da Informação é de responsabilidade de todos os colaboradores e prestadores de serviços, que devem receber uma cópia deste documento e assinar um termo de responsabilidade.

5. SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação nada mais é que um conjunto de diretrizes que definem formalmente as regras, os direitos e deveres de todos os colaboradores, visando à proteção adequada dos que compartilham a informação. Define as atribuições de cada um dos profissionais em relação à segurança dos recursos com os quais trabalham, além disso, deve prever o que pode ser feito e o que será considerado inaceitável.

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para a organização ou pessoa. Além do que está armazenado nos computadores, a informação também está impressa em relatórios, documentos, arquivos físicos, ou até mesmo repassada através de conversas nos ambientes interno e externo. Por isso, todo cuidado é pouco na hora de imprimir relatórios, jogar papéis no lixo, deixar documentos em cima da mesa, conversar sobre a empresa em locais públicos ou com pessoas estranhas ao nosso meio.

Os princípios básicos da segurança da informação são: ***confidencialidade, integridade e disponibilidade das informações***. Outras características são: irrefutabilidade, autenticação e o controle de acesso. Os benefícios são evidentes ao reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer esses princípios básicos.

- Confidencialidade: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

- Integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais;

- Disponibilidade: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

6. CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade do Diretoria/Supervisor de cada área da INDIGO DTVM estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com os critérios a seguir:

- Pública: É uma informação da INDIGO DTVM ou de seus clientes com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.

- Interna: É uma informação da INDIGO DTVM que ela não tem interesse em divulgar, onde o acesso por parte de indivíduos externos à empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da Organização, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os empregados e prestadores de serviços da INDIGO DTVM.

- Confidencial: É uma informação crítica para os negócios da INDIGO DTVM ou de seus clientes. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais à INDIGO DTVM ou aos seus clientes. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por empregados, clientes e/ou fornecedores.

- Restrita: É toda informação que pode ser acessada somente por usuários da INDIGO DTVM explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

7. SISTEMAS OPERACIONAIS

Os sistemas operacionais, ferramentas e componentes físicos são implantados e configurados pela área de TI interna.

Os sistemas possuem controle de acesso de modo a assegurar o uso apenas por usuários autorizados, mediante a validação de duplo fator de segurança (senha e código SMS). A autorização dos acessos aos sistemas deve ser claramente definida pelo supervisor da área correspondida ou diretor responsável da INDIGO DTVM, através do preenchimento do Checklist (modelo da INDIGO DTVM), e ter registrado a aprovação seja ela assinada ou via e-mail. Esse procedimento é válido para alterações/modificações de acesso e novos acessos.

Todos os sistemas possuem cópia de segurança (Backup), onde são testados e mantidos atualizados para fins de recuperação em caso de desastres.

A INDIGO DTVM mantém por 5 anos todos os logs de sistemas, e verifica regularmente, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam softwares, hardwares ou acessos que não sejam autorizados pela área de infraestrutura e Compliance.

É desabilitado aos usuários implantar novos sistemas, ferramentas e componentes básicos ou alterar quaisquer configurações sem a permissão formalizada e efetuada pela área de TI. Ainda assim, não são permitidos:

- Executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços;

- Executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da empresa;

- Enviar informações confidenciais (autorizadas) para e-mails externos sem proteção.

No mínimo, o arquivo deve contar com a proteção de uma senha “robusta” conforme descrito no item 8, controle de acesso lógico, a seguir.

8. CONTROLE DE ACESSO LÓGICO (BASEADO EM SENHAS)

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

Utilizar senha de qualidade, com pelo menos oito caracteres contendo números, letras (maiúsculas e minúsculas) e caracteres especiais (símbolos), e orienta-se que, o sistema tem proteção para que não seja possível utilizar como senha informações pessoais fáceis de serem obtidas tais como, nome, número de telefone, data de nascimento ou sequencias alfanuméricas como abcd, 1234, dentre outras.

Utilizar um método próprio para lembrar-se da senha, de modo que ela não precise ser anotada em nenhum local, em hipótese alguma.

Não incluir senhas em processos automáticos de acesso ao sistema, como por exemplo, armazenadas em macros ou teclas de função.

A distribuição de senhas aos colaboradores/usuários da INDIGO DTVM, é gerada pela área de Tecnologia da Informação de forma segura, sendo ela considerada como inicial ou não.

Todas as senhas geradas, seja ela de um novo acesso, ou quando bloqueada, é solicitado ao colaborador/usuário via sistema automatizado a alterar a senha previamente estabelecida pela TI, cadastrando uma nova senha conforme os padrões estabelecidos por TI.

Além disso, os usuários devem alterar a senha a cada 90 dias, sendo que o sistema irá enviar notificações para a alteração da mesma, 10 dias antes da expiração.

9. MÁQUINAS – ESTAÇÃO DE TRABALHO

A estação de trabalho disponibilizada para o usuário da INDIGO DTVM, tem por objetivo o desempenho das atividades profissionais do colaborador/usuário na organização.

As estações de trabalho, incluindo equipamentos portáteis, e informações estão protegidos contra danos ou perdas, bem como o acesso, uso ou exposição indevidos.

As estações de trabalho possuem códigos internos *("Nome de Host", "Ips" e etc*), os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário.

A integridade física e o perfeito funcionamento da estação de trabalho, são de responsabilidade do colaborador/usuário, seguindo as regras e orientações fornecidas pela área de infraestrutura.

São responsabilidades do usuário/colaborador:

- Encerrar a estação de trabalho no final do expediente, desligando o equipamento;
- Quando ausentar-se da mesa, o usuário/colaborador deverá bloquear a estação de trabalho e ativá-la com sua senha de acesso (Obs. Esta ação aplica-se a todos os usuários/colaboradores com estações de trabalho, incluindo equipamentos portáteis);
- Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo às entidades da INDIGO DTVM, só devem ser utilizadas em equipamentos com controles adequados.

9.1 BOAS PRÁTICAS DE SEGURANÇA PARA O NOTEBOOK

São consideradas boas práticas:

- Quando em deslocamentos de carro, coloque o mesmo no porta-malas ou em local não visível.
- Ao movimentar-se com o *notebook*, se possível, não utilize malas convencionais para *notebook* e sim mochilas ou malas discretas.
- Não coloque o *notebook* em carrinhos de aeroportos ou despache junto à bagagem.
- Em locais públicos (recepção de hotéis, restaurantes e aeroportos dentre outros), mantenha o *notebook* próximo e sempre à vista, não se distanciando do equipamento.
- Evite utilizar o *notebook* em locais públicos.
- Nos hotéis, preferencialmente, guarde o *notebook* no cofre do seu apartamento.
- Avalie se em pequenas viagens é realmente necessário levar o *notebook*.

Em caso de perda ou roubo do notebook, o usuário deverá informar imediatamente a área de T.I para que os acessos sejam bloqueados de forma remota, impedindo assim que as informações contidas no dispositivo sejam acessadas.

9.2 BOAS PRÁTICAS DE SEGURANÇA PARA IMPRESSÕES

São consideradas boas práticas para impressão de documentos:

- Todo documento enviado para a impressão, fica retido em uma fila de impressão protegida, onde o usuário libera a impressão diretamente na impressora através de senha pessoal, após a liberação do documento o mesmo deverá ser retirado imediatamente da bandeja de impressão.

- A impressão de documentos sigilosos deve ser feita sob supervisão do responsável.

9.3 BOAS PRÁTICAS DE COMUNICAÇÃO VERBAL DENTRO E FORA DA EMPRESA

São consideradas boas práticas verbais:

- Cuidado ao tratar de assuntos da empresa dentro e fora do ambiente de trabalho, em locais públicos, ou próximos a visitantes, seja ao telefone ou com algum colega, ou mesmo fornecedor.

- Evite nomes e tratativas de assuntos confidenciais, nestas situações, fora da empresa ou próximos a pessoas desconhecidas.

- Caso seja extremamente necessária a comunicação de assuntos sigilosos em ambientes públicos, ficar atento as pessoas à sua volta que poderão usar as informações com o intuito de prejudicar a imagem da empresa.

10. AQUISIÇÃO DE HARDWARES/SOFTWARES

Os procedimentos para aquisição e aprovação de Hardwares e Softwares, seguem os seguintes procedimentos e validações:

- Realizar pesquisa de mercado, dentre os fornecedores/prestadores de serviços homologados, aqueles que apresentam condições de atender às necessidades da INDIGO DTVM;

- Apresentar no mínimo 03 (três) cotações de fornecedores;

- Apresentar à diretoria o resultado das cotações/preços;

- Obter a aprovação para a aquisição do hardware/software via e-mail do diretor responsável.

- Efetuar os testes para homologação do sistema a ser adquirido, em ambiente de teste, selecionando a melhor solução a ser indicada para aquisição;

- Validar, em conjunto com os usuários, a entrada/saída de dados para garantir que eles estejam corretos e apropriados;

- Receber o software entregue pelo fornecedor, juntamente com o respectivo contrato de fornecimento e, se for o caso, o contrato de manutenção e disponibilização de novas versões e atualizações;

- Analisar o contrato e encaminhar para exame jurídico (se necessário), obtendo a aprovação e as assinaturas da diretoria;

- Encaminhar as notas ou faturas ao departamento administrativo e financeiro para o pagamento da aquisição e da manutenção mensal;

- Encaminhar a documentação relativa ao processo de aquisição ao departamento administrativo e financeiro para contabilização e para posterior arquivamento.

11. INSTALAÇÃO DE SOFTWARE E HARDWARE

Toda instalação de software e hardware deve ser feita pela Tecnologia da Informação, sendo que todos os softwares e hardwares são homologados e devidamente licenciados.

Qualquer software que, por necessidade do serviço, precisar ser instalado deverá ser comunicado a Tecnologia da Informação, para que o mesmo possa ser homologado e só assim serem disponibilizados para a área requerente.

A INDIGO DTVM respeita os direitos autorais dos softwares que utiliza e reconhece que deve pagar o justo valor por eles, não recomendando o uso de programas não licenciados nos computadores da empresa. É terminantemente proibido o uso de softwares ilegais (sem licenciamento) na INDIGO DTVM.

Toda aquisição e manutenção de sistema deve zelar pela observância dos princípios de controle sobre informações processadas e armazenadas, incluindo a adequada segregação de perfis de acesso.

Os testes de homologação são aplicados pela TI em ambiente próprio de homologação, de forma a não gerar risco de instabilidade ou interrupção nos servidores de produção.

Esses cuidados visam impossibilitar que um único colaborador domine todas as fases de controle de uma transação, ou seja, entrada, autorização, liquidação e registro da transação.

Após a aquisição e implantação do novo hardware e software, será atualizado o bem no Inventário de TI, e atualizado nos controles de licenças de software.

O equipamento deve ser configurado para instalação na rede e outros links externos, mediante a instalação dos softwares necessários.

A habilitação de usuários para uso dos softwares de rede, será realizado mediante senha de acesso.

O Compliance poderá valer-se deste instrumento para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).

12. AUTENTICAÇÃO

A autenticação é feita pelo sistema operacional Windows que implementa um conjunto padrão de protocolos de autenticação, incluindo Kerberos, NTLM, TLS/SSL e Digest, como parte de uma arquitetura extensível. Além disso, alguns protocolos são combinados com os pacotes de autenticação, como Negotiate e Credential Security Support Provider.

Estes protocolos e pacotes permitem a autenticação de usuários, computadores e serviços; o processo de autenticação, por sua vez, permite que os usuários e os serviços autorizados acessem recursos de forma segura e limitada de acordo com a necessidade e permissão do colaborador.

A mesma senha para acesso ao S.O./REDE libera acesso à Internet por meio da integração Firewall/AD. Seguindo todas as regras de filtros de conteúdo de internet.

13. CRIPTOGRAFIA

A rede INDIGO DTVM utiliza criptografia em um local central seguro (AD), tornado o processo de autenticação escalonável. Active Directory é uma tecnologia padrão para armazenar informações de identidade, que incluem a criptografia chaves que são as credenciais do usuário. Active Directory é necessário para implementações de Kerberos e NTLM padrão.

Para as redes Wifi, é utilizado: WPA2, protocolos como o RADIUS, 802.1x, EAP. TKP, AES e RSN (Robust Security Network) e oferece os modos de operação Enterprise (Infraestrutura) e Personal (Preshared Key). A Rede Wifi é totalmente apartada da rede local LAN.

13.1 PREVENÇÃO E A DETECÇÃO DE INTRUSÃO

São realizadas periodicamente manutenções e atualizações técnicas e de segurança, de forma a manter em plenas condições de funcionamento, os equipamentos de informática e de telecomunicações. Testes nos sistemas de Firewall, visam aumentar a segurança e eliminar possíveis vulnerabilidades, além das estações terem sistema de antivírus atualizado e patchs de correção são aplicadas de acordo com a disponibilização.

13.2 COMPARTILHAMENTO DE INFORMAÇÕES SOBRE INCIDENTES RELEVANTES

A INDIGO DTVM disponibilizará as informações sobre os seus incidentes relevantes, em especial, seus registros, análises da causa e do impacto e os controles dos efeitos dos incidentes com as demais instituições financeiras e autorizadas a funcionar pelo Banco Central do Brasil por meio das iniciativas ajustadas entre as instituições, resguardando sempre o sigilo bancário das informações, seus segredos de negócios e privilegiando a livre concorrência entre os participantes do mercado.

13.3 PREVENÇÃO DE VAZAMENTO DE INFORMAÇÕES

Todo acesso às informações e aos ambientes lógicos deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas. As autorizações são revistas, confirmadas e registradas periodicamente ou conforme mudanças de funcionários.

Somente a diretoria da INDIGO DTVM pode autorizar a divulgação pública de informações dos diversos setores, independentemente do canal de comunicação: mídia impressa, eletrônica ou qualquer outro meio.

O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado. Os dados, as informações e os sistemas de informação das entidades devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens.

Toda informação relevante deverá ser protegida, de acordo com seu grau de sigilo, integridade e disponibilidade, de forma a atender aos objetivos de segurança da informação.

13.4 TESTES E VARREDURAS PARA DETECÇÃO DE VULNERABILIDADES

Todo sistema computadorizado possui diversas entradas e saídas lógicas disponíveis para a comunicação entre seus próprios componentes ou aplicações externas.

Por outro lado, o aumento do uso de tais ferramentas potencializa os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integridade e a disponibilidade dos dados ou dos sistemas das instituições.

Existem diversas razões para que esses ataques sejam realizados por vários agentes (organizações criminosas ou *hackers* individuais, organismos de Estado, terroristas, colaboradores, competidores etc.). Os principais motivos identificados são:

- Obter ganho financeiro;
- Roubar, manipular ou adulterar informações;
- Obter vantagens competitivas e informações confidenciais de empresas concorrentes;
- Fraudar, sabotar ou expor a instituição invadida, podendo ter como motivo acessório a vingança;

- Promover ideias políticas e/ou sociais;
- Enfrentar desafios e/ou ter adoração por hackers famosos.

Os invasores podem utilizar vários métodos para os ataques cibernéticos. Destacam-se os mais comuns:

- *Malware* - *softwares* desenvolvidos para corromper computadores e redes:

Vírus: *software* que causa danos ao computador, rede, *softwares* e banco de dados.

Cavalo de Troia: aparece dentro de outro *software* e cria uma porta para a invasão do computador.

Spyware: software malicioso para coletar e monitorar o uso de informações.

Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

- Engenharia social - métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:

Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento.

Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais.

Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais.

Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais.

Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

- Ataques de DDoS *(distributed denial of services)* e *botnets:* ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição, no caso dos *botnets,* o ataque vem de muitos computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

- Invasões (*advanced persistent threats*) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

A análise de vulnerabilidade é um dos itens fundamentais no gerenciamento de risco, pois de forma frequente são verificadas as vulnerabilidades ou exposições existentes.

As principais vantagens nas atividades da análise de vulnerabilidade são:

• Identificação das vulnerabilidades;
• Correção das vulnerabilidades reduzindo os riscos;
• Mapeamento proativo das ameaças existentes;
• Redução no tempo de paradas;
• Economia de recursos;
• Maior controle sobre os potenciais de riscos.

O objetivo da análise de vulnerabilidade é reduzir o risco em relação aos incidentes de segurança, seja tanto na rede interna quanto na externa, é necessário detectar essas possíveis falhas e corrigi-las para garantir que a rede esteja em um nível de segurança adequada.

A análise de vulnerabilidade visa detectar falhas em diversos componentes como: aplicações, softwares, equipamentos, sistemas operacionais, dentre outros. Deve-se fazer continuamente o processo de verificação e análise da rede, para que a mesma fique sempre atualizada e livre de acessos não permitidos e indesejáveis.

Essa análise é feita de forma remota por empresa de segurança parceira da INDIGO DTVM.

Os testes de invasão ou vulnerabilidade têm como objetivo descobrir e explorar falhas de segurança, permitindo assim que pontos de vulnerabilidade sejam identificados e corrigidos de forma antecipada.

O teste de invasão realizado, faz-se uso de todos os artifícios que um hacker geralmente usaria. Em outras palavras, o que se tem são simulações controladas de ataques reais, objetivando a avaliação da segurança da organização e relatando as deficiências tanto da estrutura física quanto lógica para que possam ser corrigidos.

O teste de invasão envolve análise de rede e de portas, identificação de sistemas, vulnerabilidades em sistemas sem fios, verificação de serviços (como site da empresa, correio interno, servidor de nomes e documentos visíveis), determinação de vulnerabilidades e identificação dos exploits, verificação manual das vulnerabilidades, verificação das aplicações, verificação de firewall, revisão das políticas de segurança, verificação

de sistemas de detecção de intrusos, revisão de sistemas de telefonia, obtenção de informação sobre a empresa, engenharia social, verificação de sistemas considerados confiáveis, análise de senhas, revisão da política de privacidade, análise de cookies e bugs no site, revisão de arquivos de log e até mesmo análise do lixo corporativo.

13.5 PROTEÇÃO CONTRA SOFTWARES MALICIOSOS

A INDIGO DTVM mantém sistemas confiáveis mediante utilização de padrões tecnológicos de segurança de rede, para evitar fraudes internas e invasões e garantir o sigilo de toda informação e comunicação interna e externa, testes diários são realizados nas estações de trabalho de forma automática.

13.6 ANTÍVIRUS

Antivírus dos servidores e estações são atualizados automaticamente e a varredura por vírus é feita diariamente nas estações e servidores.

A INDIGO DTVM utiliza a ferramenta de endpoint da SOPHOS, configurada e gerenciada pela equipe interna de T.I.

13.7 ESTABELECIMENTO DE MECANISMOS DE RASTRABILIDADE

Todo usuário é adequadamente identificado, sendo responsável pela utilização do equipamento no desempenho de suas atividades diárias.

Os *softwares* referentes aos controles de ativo e passivo, possuem trilha de auditoria para assegurar o rastreamento de eventos, possibilitando:

- Identificação do usuário;
- Data e horário de ocorrência do evento;
- Identificação do evento (inclusão, alteração ou exclusão).

No caso da rede interna de computadores, são utilizadas trilhas de auditoria com os seguintes registros de acessos: usuário, data e horário.

No caso do compartilhamento de arquivos (Sharepoint) são utilizadas trilhas de auditoria com os seguintes registros: e-mail do usuário, data, horário e qual evento realizado (inclusão, alteração ou exclusão).

13.8 CONTROLES DE ACESSO E DE SEGMENTAÇÃO DA REDE DE COMPUTADORES

São utilizados equipamentos de rede que possibilitam a segmentação e/ou integração com outras redes, facilitando essas interligações, preservando segregado os interesses de tráfego de cada rede e evitando o congestionamento e outros efeitos que possam prejudicar seu desempenho.

As máquinas (servidores) que armazenam sistemas da INDIGO DTVM estão em área protegida com softwares, firewalls, antivírus, autenticação/criptografia.

A entrada aos Data Centers tem acesso devidamente controlado e monitorado.

A entrada nestas áreas ou partes dedicadas, por pessoas não autorizadas (visitantes, prestadores de serviço, terceiros e até mesmo funcionários, sem acesso liberado), que necessitarem ter acesso físico ao local, sempre o farão acompanhados de pessoas autorizadas.

O acesso às dependências da empresa com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só pode ser feito a partir de autorização da Diretoria e mediante supervisão. Exceto para eventos e treinamentos organizados pela própria empresa.

Respeitar áreas de acesso restrito, não executando tentativas de acesso às mesmas, ou utilizando máquinas alheias às permissões de acesso delimitadas a cada categoria de colaboradores.

14. UTILIZAÇÃO DE EQUIPAMENTOS PARTICULARES

Notebooks particulares/terceiros para serem usados dentro da rede, precisam ser avaliados pela TI.

Equipamentos de terceiros devem ser levados ao suporte para serem verificadas atualização do antivírus e existência de vírus.

É de responsabilidade da área contratante encaminhar os terceiros para esta verificação.

Nenhum equipamento de terceiro é conectado a rede da INDIGO DTVM, tais equipamentos utilizam somente a rede de Clientes/Visitantes que, é totalmente apartada da rede LAN.

15. UTILIZAÇÃO DA REDE CORPORATIVA

Material em desacordo com a Política de Compliance não pode ser explícito, armazenado, distribuído, editado ou gravado através de uso dos recursos computacionais da rede corporativa.

A TI deverá estabelecer os aspectos de controle, distribuição e instalação de softwares utilizados.

Somente os diretores e/ou colaboradores previamente autorizados, podem falar em nome da INDIGO DTVM para os meios de comunicação. Em caso de dúvidas, procurar a Diretoria.

Todos os arquivos são gravados na rede, arquivos gravados no computador (local) são automaticamente sincronizados para a ferramenta homologada pela área de T.I que é o Onedrive da Microsoft. O espaço em disco e em nuvem corporativa é controlado por departamento, por isso, os usuários devem administrar seus arquivos gravados, excluindo os arquivos desnecessários.

Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos, etc..) nos drivers de rede, pois ocupam espaço comum limitado dos departamentos.

16. USO DE MÍDIAS REMOVÍVEIS E PORTA USB

O uso de mídias removíveis na INDIGO DTVM não é permitido, devendo ser tratado como exceção à regra.

A porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais, nesse caso, os modens 3G e pen drive merecem especial atenção. Tal vulnerabilidade não pode ser contida com *firewalls* ou com programas antivírus já que os dispositivos são acoplados aos equipamentos pelos próprios funcionários da empresa.

O uso de portas USB dos desktops e notebooks é bloqueado por padrão via GPO de segurança, caso haja necessidade de uso, se faz necessário justificar tal necessidade e obter aprovação da área de Compliance. Para notebooks de Coordenadores e cargos acima, esta liberação é efetuada por padrão.

17. USO DA INTERNET

A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à empresa.

O acesso às páginas e web sites é de responsabilidade de cada usuário, ficando vedado o acesso a sites com conteúdo impróprio e páginas de relacionamento.

Os acessos à internet são monitorados através de identificação e autenticação do usuário.

Os sistemas de controle de acesso as páginas da web possuem bloqueio de sites impróprios por regras de firewall e blacklist.

18. RECOMENDAÇÕES SOBRE O USO DE E-MAIL

É vedado o uso de sistemas webmail externo. O uso do correio eletrônico para envio e recepção de e-mail deverá ocorrer apenas através do correio eletrônico da INDIGO DTVM.

É proibido o uso do Correio Eletrônico para envio de mensagens que possam comprometer a imagem da empresa perante seus clientes e a comunidade em geral e que possam causar prejuízo moral e financeiro.

Evitar utilizar o e-mail da empresa para assuntos pessoais.

Assegurar a propriedade de todas as mensagens geradas internamente e/ou por meio de recursos de comunicação e definir o uso desses recursos como ferramenta de comunicação e aumento de produtividade, 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.

Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas: .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela área de TI.

Não utilizar o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não reenviando e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/Symantec, criança desaparecida, criança doente, materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais, etc.

Utilizar o e-mail para comunicações oficiais internas, as quais não necessitem obrigatoriamente do meio físico escrito. Isto diminui custo com impressão e aumenta a agilidade na entrega e leitura do documento.

A utilização do e-mail/webmail da empresa fora do horário de trabalho para posições que possuam controle/reporte de jornada deve ser aprovado pelo Diretor da área.

19. SEGURANÇA FÍSICA

Os colaboradores da INDIGO DTVM vão utilizar a senha biométrica para acesso aos ambientes do CPD visando evitar acessos indevidos por pessoas não autorizadas nas dependências do mesmo.

Os colaboradores e prestadores de serviços de manutenção são autorizados a acessar o ambiente de CPD somente mediante acompanhamento de funcionário de TI.

As máquinas (servidores) que armazenam sistemas da INDIGO DTVM estão em áreas
protegidas– CPD localizado na empresa, com redundância, em ambiente climatizado.

A entrada ao CPD tem acesso devidamente controlado e monitorado.

A entrada nestas áreas ou partes dedicadas, por pessoas não autorizadas (visitantes, prestadores de serviço, terceiros e até mesmo funcionários, sem acesso liberado), que necessitarem ter acesso físico ao local, sempre o farão acompanhados de pessoas autorizadas.

O acesso às dependências da empresa com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só pode ser feito a partir de autorização da Diretoria da INDIGO DTVM e mediante supervisão. Exceto para eventos e treinamentos organizados pela própria empresa.

Respeitar áreas de acesso restrito, não executando tentativas de acesso às mesmas, ou utilizando máquinas alheias às permissões de acesso delimitadas a cada categoria de colaboradores.

20. SEGURANÇA LÓGICA

A segurança lógica permite que o acesso virtual a dados e informações da organização, de acordo com as necessidades específicas de cada departamento

A identificação e autenticação dos usuários para acesso à rede, arquivos e sistemas da INDIGO INVESTIMENTOS é sempre por processo de login com critérios de segurança já especificados nesta política.

Os links de comunicação com a web são monitorados por um sistema contratado onde, através do monitoramento ativo, relatórios de vulnerabilidades são gerados e a equipe de T.I pode identificar prontamente possíveis problemas internos e externos, para assim, tomar as medidas necessárias e reduzir os incidentes relacionados a ao ambiente cibernético. A verificação periódica dos testes e varreduras para detecção de vulnerabilidades atendem os requisitos obrigatórios da resolução 4893 do BACEN

Um sistema de Firewall de borda realiza uma camada de proteção contra conteúdos maliciosos, fraudulentos e monitora canais seguros de comunicação. Através de um conjunto de regras, o tráfego de rede é inspecionado e protegido contra;

• Malwares (Bots, Vírus, Worms, Backdoors e Trojan Horses)
• Ataques (DDoS, Portscans, IP Spoof e ARP Spoof)
• Anomalias no tráfego de rede (fragmentação de pacotes)
• Detecção de Aplicações de Rede (VPN´s, Proxys, Softwares de acesso remoto, p2p, torrente e hacktools)

21. SEGURANÇA NA COMUNICAÇÃO DE DADOS DE VOZ

A INDIGO DTVM em conformidade com legislação vigente mantém sistema de gravações das comunicações feitas pelos seus colaboradores que utilizam os equipamentos e instalações, visando preservar a INDIGO DTVM no caso de eventuais ações dolosas ou contrárias a seus interesses comerciais e/ou operacionais.

As instalações e equipamentos de comunicação de dados e voz são gerenciados de modo a que seja mantida a segurança e inviolabilidade das informações que trafegam por elas.

As gravações e rotinas de monitoramento serão feitas com base em concordância expressa dos colaboradores mediante adesão e assinatura de Termo de Compromisso e Responsabilidade e Compromisso, o mesmo deve ser assinado pelo colaborador no início de suas atividades na INDIGO DTVM.

A manutenção da infraestrutura de comunicações envolve:

- Telefonia VOIP
- Links de contingência, com LoadBalance;
- Ambiente de rede de dados;
- Sistemas de gravação de voz.

A Segurança da Informação dispõe de meios para garantir a não interrupção das comunicações, efetuar o monitoramento do desempenho dos *links* de dados, adotar providências internas junto às concessionárias para melhoria do desempenho e corrigir eventuais problemas.

22. SEGURANÇA DE HARDWARE

O isolamento físico e o controle do acesso compõem a nossa base de segurança tanto dos terminais quanto dos servidores. Garantindo que os equipamentos estejam instalados em um ambiente seguro e protegido contra o acesso não autorizado, com os devidos termos de concessão de acesso e Biometria que libera a trava de segurança.

Da mesma forma, os registros de acesso e a série dos equipamentos ajudam a evitar o uso não autorizado. Também é feito o controle via GPO de segurança para que os terminais não tenham acesso a mídias removíveis; como por exemplo: PenDrive, CDs e etc.

23. SEGURANÇA DE SOFTWARE

O *software* de prevenção contra vírus está instalado na rede interna e nas estações de trabalho, com rotinas de varredura, atualizações e prevenções contra invasões e vazamentos de informações.

O uso do correio eletrônico e Internet pelos colaboradores é monitorado não sendo permitido acesso a sites não autorizados, e está sujeito a restrições no recebimento de arquivos anexados.

Os servidores/terminais com acesso à internet e e-mail dispõem de *firewall* e ferramentas de segurança de rede.

24. NORMAS DE BACKUP

Foram estabelecidas as seguintes regras quanto à realização de *backups*:

- Geração diária e incremental de cópias de segurança;
- Inclusão de todas as informações armazenadas nos servidores;
- A base de dados é salva e gravada no servidor em nuvem.

O ambiente do CPD possui termômetro para marcação de temperatura, umidade, detecção de fumaça com alarme de emergência, software de monitoramento e relativas. Os equipamentos estão instalados em locais adequados, protegidos dos raios solares, de altas temperaturas e de grande incidência de pó.

Os servidores e os equipamentos instalados na sala de informática são protegidos da falta de energia elétrica por *nobreaks* que garantem:

- A uniformidade da tensão da rede, em casos de picos de energia;
- A entrada em operação das baterias, na falta de energia elétrica, com autonomia de cerca de 3 horas.

Os servidores estão instalados em sala exclusiva, climatizada, dotada de detector de fumaça e terá permissão de acesso apenas às pessoas autorizadas com trava biométrica.

25. TESTE DE RESTORE

- O teste de “Restore” é um procedimento periódico feito em média uma vez por mês.
- A documentação está armazenada em Atas dividido por dada de teste.
- As Atas estão salvas na REDE junto as documentações de Backup e P.S.I.

26. CONTRATAÇÃO DE SERVIÇOS

Observar os procedimentos quanto ao recebimento da solicitação do usuário. Selecionar dentre os prestadores de serviços homologados, no mínimo 3 (três) empresas, obtendo as respectivas propostas.

Analisar as propostas em conjunto com os usuários/diretoria e adotar os procedimentos previstos para contratação do serviço, pagamento e arquivamento da documentação.

27. CONFIGURAÇÕES DE SENHAS

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

Utilizar um método próprio para lembrar-se da senha, de modo que ela não precise ser anotada em nenhum local, em hipótese alguma.

O padrão de segurança ser adotados nos sistemas e rede para utilização da senha pelo usuário:

- Tempo limite sem utilização do Sistema o parâmetro adotado foi de 90 dias;
- Número Máximo de Tentativas de Acesso ao Sistema, 3 tentativas.
- Não conter sequencias lógicas (por exemplo. 1234, abcd, aeiou)

Os pré-requisitos de segurança para definição/utilização da senha dos usuários, são:

- Não conter o nome da conta ou mais de dois caracteres consecutivos de partes do nome completo do usuário
- Ter pelo menos seis caracteres
- Conter caracteres de três destas quatro categorias:
- Maiúsculos (A-Z)
- Minúsculos (a-z)
- Dígitos de base 10 (0 a 9)
- Não alfabéticos (por exemplo, !, $, #, %)

Os requisitos de complexidade são impostos quando as senhas são alteradas ou criadas.

28. MONITORAMENTO

Todos os ramais dos colaboradores do escritório da INDIGO DTVM são gravados, sendo realizado monitoramento semanal para verificação do funcionamento dos equipamentos e análise por amostragem das gravações efetuadas nas mesas.

A mesma política de gravação é feita em canais de conferência para quando os dirigentes utilizam os canais para reuniões.

29. GESTÃO DE INCIDENTES

A gestão de incidentes em é um conjunto de boas práticas que visam a manutenção, operação e infraestrutura dos serviços de TI da INDIGO DTVM. Esse cuidado se aplica não só aos setores operacionais, mas também aos setores estratégicos da Indigo.

A área de Segurança da Informação realiza a monitoração de segurança do ambiente tecnológico da INDIGO DTVM, analisando os eventos e alertas com o objetivo de identificar possíveis incidentes. Os incidentes que são identificados pelos alertas são classificados com relação ao impacto de acordo com os critérios adotados pela Indigo. Para o seu grau de relevância serão considerados aspectos como comprometimento de dados de clientes e impacto ao sistema financeiro.

Todos os incidentes passam por um processo de tratamento e comunicação, onde são registradas todas as informações pertinentes aos incidentes como causa, impacto, classificação etc., de acordo com o procedimento operacional.

Visando aprimorar a capacidade da Indigo na resposta a incidentes cibernéticos, alguns cenários que possam afetar a continuidade de negócios são considerados nos testes. Os incidentes de Segurança da Informação e cibernéticos da Indigo devem ser reportados à Segurança da Informação, a área de Segurança elaborará um Relatório Anual contendo os incidentes relevantes ocorridos no período, ações realizadas de prevenção e respostas aos incidentes e resultados dos testes de continuidade. Este relatório deverá ser apresentado ao Comitê de Risco e ao Conselho de Administração, conforme determinações legais e regulamentares.

30. PRINCÍPIOS E DIRETRIZES DE SEGURANÇA

A INDIGO DTVM promove a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e treinamentos de capacitação realizados anualmente, com o objetivo de fortalecer a cultura de Segurança da Informação e a conscientização dos usuários. Os treinamentos de capacitação dos usuários são realizados na modalidade on-line, abordando assuntos relacionados a confidencialidade, integridade e disponibilidade da informação.

Estas campanhas são veiculadas através de grupos de treinamentos no Microsoft Teams divididos em grupos de até 8 pessoas, todo o conteúdo do treinamento é disponibilizado aos colaboradores e parceiros.

Todos os colaboradores são orientados a realizar o treinamento e ao término da capacitação, a Indigo disponibiliza um certificado de participação.

31. COMPROMISSO DA ALTA ADMINISTRAÇÃO

A alta administração contribui continuamente para o fortalecimento do Sistema de Controles Internos e da Segurança Cibernética, se comprometendo no mínimo, mas não se limitando as ações abaixo:

- Investir recursos necessários ao processo de prevenção de incidentes;
- Incentivar e praticar continuamente a disseminação de uma cultura de controles internos e de gestão de riscos;

- Manter colaboradores experientes, qualificados, motivados, continuamente treinados e comprometidos com suas atribuições e responsabilidades; com os objetivos e metas estabelecidos pela administração e com a prestação de serviços de qualidade; e

- Incentivar a segregação de funções nas diversas áreas envolvidas no processo de prestação desses serviços.

32. CONTROLE DE DESENVOLVIMENTOS INTERNOS

Todas as atividades de desenvolvimento e manutenções de sistemas executadas pela equipe interna está sujeita às políticas, padrões, procedimentos e outras convenções de desenvolvimento. Os sistemas desenvolvidos internamente ou desenvolvidos para atender a INDIGO DTVM deverão, em sua fase de homologação, passar por uma avaliação de segurança com o objetivo de identificar possíveis vulnerabilidades ou desvios dos controles de segurança.

Os ambientes de desenvolvimento e produção devem ser segregados por um ambiente de testes, de forma que as aplicações desenvolvidas ou adquiridas não entrem em produção sem estar devidamente testadas e documentadas. Desta forma, devem ser implementados controles apropriados para garantir a inexistência de conflito de funções quando do desenvolvimento, manutenção e promoção de sistemas para o ambiente de produção. Os ambientes de desenvolvimento e produção devem ser segregados por um ambiente de testes, de forma que as aplicações desenvolvidas ou adquiridas não entrem em produção sem estar devidamente testadas e documentadas.

Os colaboradores das áreas de desenvolvimento, homologação e produção não podem executar funções em duas dessas três áreas ao mesmo tempo. Isto somente estará autorizado, caso o colaborador mude oficialmente de área e após a certificação de que este colaborador não carrega nenhum acesso da antiga área.

33. BOAS PRÁTICAS CONTRATAÇÃO SERVIÇO DE COMPUTAÇÃO EM NUVEM

A INDIGO INVESTIMENTOS utiliza de Infraestrutura como serviço (IaaS – Infrastructure as a Service) onde executamos nossas aplicações na infraestrutura de nuvem do provedor.

Critérios para a contratação são avaliados pela equipe de T.I interna como

- Nuvem gerenciada
- Classificação de data centers em Tiers de acordo com a norma TIA 942
- Rápida elasticidade:
- Resiliência. Baixo potencial de falha e o risco de downtime
- Capacidade do fornecedor
- SLA (Service Level Agreement) de atendimento e disponibilidade dos serviços
- Redundância de datacenters
- Due Diligence