POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Introdução e Objetivo

A segurança da informação é um dos assuntos mais importantes dentre as preocupações de qualquer empresa. Confidencialidade, integridade e disponibilidade da informação estão diretamente ligadas à segurança. Os dados são considerados um dos principais patrimônios de uma organização, e os mesmos estão sob constante risco. A sua perda ou roubo constitui um prejuízo para a estratégia do negócio.

Com objetivo de minimizar esses riscos, elaboramos uma Política Segurança da Informação que tem como objetivo estabelecer princípios e diretrizes de proteção das informações, proteção contra ameaças cibernéticas, considerando a confidencialidade, integridade e disponibilidade para mitigar casos de incidentes de segurança visando minimizar os impactos aos objetivos estratégicos Equitas Investimentos.

Adicionalmente, descrever as normas de utilização e atividades consideradas violação ao uso dos serviços e recursos de TI da Equitas, tais como, mas não limitado a, computadores, e-mails do domínio EQUITAS.com.br, acessos remotos, link de Internet, espaço em rede e afins.

A área de Compliance e Equipe de Infra/Segurança constituem um fórum de "Segurança da Informação" e reúne-se de forma extraordinária, sempre que convocado por qualquer de seus membros. Todos os assuntos discutidos serão reportados ao Comitê de Compliance em suas reuniões ordinárias.

Abrangência

Todos os colaboradores e partes interessadas da Equitas Investimentos que tenham acesso concedido às informações, em qualquer meio (física e/ou eletrônica), ou aos sistemas e recursos computacionais estão sujeitos a essa política, independentemente do nível hierárquico.

Para os fins do disposto nesta política, o termo "Colaboradores" abrange todos os sócios, funcionários, menores aprendizes, estagiários e prestadores de serviços da Equitas.

Conceito e definições

Informação: é um ativo que tem um valor para a organização e, consequentemente necessita ser adequadamente protegida. A informação pode existir de diversas formas: impressa ou escrita, armazenada eletronicamente, transmitida pelo correio ou falada em conversas. Seja qual for a forma pela qual a mesma é apresentada, transmitida, armazenada ou compartilhada, é recomendado que a mesma seja protegida adequadamente.

Segurança da Informação: protege a informação de diversas ameaças para garantir a integridade, confidencialidade e disponibilidade para a proteção e continuidade dos negócios.

Política de Segurança: é uma série de normas internas padronizadas pela empresa que devem ser seguidas para que todas as possíveis ameaças sejam minimizadas e combatidas de forma eficaz.

Dispositivos TI: Entende-se como Dispositivos de TI todo equipamento conectado direto ou indiretamente a Rede Local seja via Cabo, Wireless ou Internet, sendo mais comuns dos tipos desktop, notebook, smartphone, tablets e etc. Estes equipamentos deverão seguir procedimentos e regras definidos pela Equitas.

Confidencialidade: É a garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Integridade: É a garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

Disponibilidade: É garantia de que os usuários/sistemas autorizados obtenham acesso às informações e aos ativos correspondentes sempre que necessário.

Informações Confidenciais: são aquelas não disponíveis ao público, que: (a) identifiquem dados pessoais ou patrimoniais (b) sejam objeto de acordo de confidencialidade celebrado com terceiros (c) identifiquem ações estratégicas cuja divulgação possa prejudicar a gestão dos negócios ou reduzir sua vantagem competitiva (d) autenticação de sua identidade (senhas de acesso ou crachás) de uso pessoal e intransferível.

Ataque cibernético: é uma ação praticada por hackers que consiste na transmissão de vírus (arquivos maliciosos) que infectam, danificam e roubam informações de computadores e demais bancos de dados online. Os ataques cibernéticos mais comuns são:

Malware: softwares desenvolvidos para corromper computadores e redes: (i) Vírus: software que causa danos a máquina, rede, softwares e banco de dados; (ii) Cavalo de Troia: aparece dentro de outro software e cria uma porta para a invasão do computador; (iii) Spyware: software malicioso para coletar e monitorar o uso de informações; e (iv) 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: (i) Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento; (ii) Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais; (iii) Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais; (iv) Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e (v) 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.

Invasões: ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Teste de Invasão – Simular um ataque de hacker para identificar vulnerabilidades em sistema, softwares e infraestrutura que suporta o negócio da Equitas.

Classificação da informação

As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Confidencial, Pública e Restrita.

Informações Confidenciais: são aquelas que o conhecimento, acesso e a modificação estão restritos a um grupo seleto, havendo necessidade de possuírem controles de segurança que garantam a proteção dos pilares de segurança da informação (confidencialidade, integridade e disponibilidade).

Informação Pública: são aquelas que podem ser divulgadas a qualquer pessoa ou empresa, onde não proporciona impacto ao negócio da Equitas.

Informação Restrita: são aquelas que, em razão de lei, interesse público ou para a preservação de direitos e privacidade de dados, devam ser de conhecimento reservado e, portanto, requeiram medidas especiais para sua segurança e salvaguarda.

Deve ser atribuída a classificação mais restritiva ao documento que contiver as informações de diferentes graus de confidencialidade. O documento deve ser classificado como sigiloso ou confidencial. Essa regra se aplica para o caso de documento que não pode ser dividido para fins de acesso.

A Equitas considera como informações restritas, focado na privacidade dos dados:

Número de CPF
Data de Nascimento;
Número de Passaporte;
Informações de conta corrente
Número de Telefones;
Logradouro
Informações Financeiras;
Saldos de investimentos
Número de CNH
Número de Identidade

Diretrizes

As diretrizes estão divididas nos seguintes tópicos:

- Criação de Senhas
- Sistemas de Segurança
- Utilização da Rede
- Utilização de E-Mail
- Utilização de acesso à Internet
- Utilização de impressoras/Documentos
- Manutenção/Chamados Técnicos

CRIAÇÃO DE SENHAS

A criação de senha visa assegurar a utilização de forma correta dos dispositivos de TI que os usuários terão acesso. Uma senha segura deverá conter no mínimo 8 caracteres alfanuméricos (letras e números) de preferência com alternância entre maiúscula e minúscula. Padrão de Senhas:

- Mínimo 8 caracteres;
- Não utilizar na senha nomes, sobrenomes, apelidos, datas, número de telefones e palavras constantes em dicionários mesmo que idiomas diferentes;
- A senha de rede deverá ser alfanumérica misturando letras e números;
- As senhas deverão ser trocadas a cada 90 dias;
- Não poderão ser reutilizadas senhas antigas, as mesmas serão bloqueadas por um período pré-determinado pela Equipe de Infra/Segurança;

Para facilitar a memorização das senhas, utilize padrões mnemônicos com a elaboração de frases que possibilitam sua fácil memorização. As senhas terão um tempo de vida útil pré-determinado pela Equipe de Infra/Segurança, devendo o mesmo ser respeitado, caso contrário o usuário ficará sem acesso.

Regras para utilização de senhas:

- Sua senha é pessoal e intransferível, não devendo ser repassada a ninguém, nem mesmo à Equipe de Infra/Segurança. Em casos de qualquer incidente de segurança solicitamos a troca imediata de suas senhas;
- O uso da senha será de total responsabilidade do proprietário da senha, respondendo por qualquer penalidade por uso indevido;
- Não anote a senha em papel, post-it e etc., para evitar que outras pessoas tenham acesso aos seus dados de logon;
- Caso a senha seja digitada errada após 5 (cinco) tentativas, a mesma será bloqueada. Seu desbloqueio deverá ser solicitado à Equipe de Infra/Segurança da Equitas;
- Não utilizar a mesma informação de autenticação secreta (login e senha) para uso profissional e pessoal.

A solicitação de *reset* de senhas deverá ser efetuada somente através do Help Desk – helpdesk@netonze.com.br. A equipe de Infra/Segurança poderá a qualquer momento efetuar o bloqueio de acesso sem prévio aviso sempre que identificar uma possível violação à Política de Segurança.

SISTEMAS DE SEGURANÇA

A Gestora adotada de um conjunto de Sistemas de Segurança que visam garantir um nível de segurança às informações pertinentes à Equitas, seus Clientes, Parceiros, Fornecedores e etc.

Em um âmbito geral (Rede) a EQUITAS adota os seguintes sistemas:

- Firewall com Diferentes Camadas;
- DMZ;
- IDS / HIDS;
- VPN;
- Proxy;
- Proxy Reverso;
- Sistemas de Antivírus;
- Sistemas de Backup;
- Sistemas Críticos com Redundância;
- Sistemas de Contingenciamento de Energia;
- Segurança Física (Acesso, Monitoramento, Rede);

No ambiente das Estações, podemos destacar a utilização dos sistemas de:

Firewall Pessoal

Firewall é um sistema de proteção contra ataques a serviços instalados bloqueando acessos não autorizados ao seu computador.

Sua configuração está autorizada apenas à equipe de Infra/Segurança não devendo o usuário efetuar qualquer alteração ou desativação do serviço.

Além do Firewall dos computadores, existem outros níveis de Firewalls na rede que controlam o acesso de / para determinados locais internos e externos. Esses sistemas são transparentes e monitorados como forma de auditoria e controle de acesso.

Antivírus

Antivírus é um sistema que efetua a verificação de arquivos, e-mails e etc. à procura de qualquer código malicioso que possa ser identificado como uma ameaça ao sistema. Atualmente temos homologado o sistema de Antivírus da McAfee para as Estações e Servidores de Rede, além do Clamav e Symantec para os sistemas de E-mail e Internet.

A Verificação pelo antivírus ocorre:

- Nos Servidores;
- Na navegação de Internet e E-mail;

- Nas Estações na execução de arquivos e programas;
- No envio/recebimento de e-mails do Outlook;

Além da execução nesses níveis, o Antivírus está programado para efetuar uma varredura completa no sistema, semanalmente. Essa verificação não poderá ser cancelada ou sofrer qualquer interferência pelo usuário.

Para um funcionamento correto do Antivírus o mesmo deverá estar atualizado, constantemente. Para isso existe uma rotina de atualização que é efetuada todos os dias por volta das 12:00 hs.

Em caso de detecção ou suspeita de qualquer anomalia no sistema, o usuário deverá contatar imediatamente a equipe de Infra/Segurança que fará uma verificação completa em todo o sistema e avaliará se e quais danos foram causados pela infecção.

Além das programações de checagem de vírus, existe uma análise que é efetuada mensalmente com a verificação completa do sistema utilizando 3 diferentes Antivírus para assegurar a total imunização do sistema.

A equipe de Infra/Segurança poderá solicitar acesso a qualquer computador para efetuar uma verificação, sempre que suspeitar de infecção do sistema.

AntiSpyWare

AntiSpyware é um sistema de proteção contra programas espiões que possam infectar o sistema com a finalidade de coletar informações pessoais e dados sigilosos do usuário. Atualmente, utilizamos os sistemas Windows Defender, Spyboot e Ad-Aware para proteção dos sistemas nas estações.

Esses sistemas estão programados da seguinte forma:

- Checagem OnLine através do Windows Defender;
- Checagem Semanal através do Windows Defender;
- Checagem Mensal através do Spyboot;

Além das checagens programadas, existe a checagem manual que é efetuada mensalmente através do programa de manutenção executado pela equipe de Infra/Segurança.

AntiSpam

O AntiSpam é um sistema que efetua uma análise nos e-mails recebidos classificando os mesmos como possível lixo eletrônico (propaganda, e-mails falsos, correntes e etc), efetuando uma classificação e filtragem para otimizar o serviço de e-mail da empresa. Atualmente, executamos a análise de AntiSpam em 5 (cinco) níveis de proteção.

Atualizações Automáticas

As Atualizações Automáticas são programas para efetuar a atualização e correção do sistema Operacional e softwares básicos instalados a fim de corrigir possíveis falhas do software. Essa atualização é efetuada automaticamente pelo próprio sistema e não necessita de interferência do usuário.
Caso ocorra alguma correção crítica que a equipe de Infra/Segurança avalie como necessária, será efetuada intervenção na máquina do usuário e a atualização será executada.

Manutenção Preventiva

Além dos sistemas de segurança implantados, a equipe de Infra/Segurança efetuará, periodicamente, manutenção preventiva em todos os sistemas, a fim de garantir o perfeito funcionamento e a integridade completa do sistema.

Essa manutenção ocorrerá pelo menos 1 vez por mês e tem como características:

- Checagem/Atualização dos sistemas instalados;
- Verificação manual dos Antivírus através de 3 Antivírus diferentes (McAfee, BitDefender, Panda). Caso seja encontrado algum arquivo infectado, será executado adicionalmente, o Antivírus Trend até que seja eliminado o vírus;
- Verificação manual dos AntiSpywares através do BitDefender, Spybot e Ad-Aware;
- Verificação do registro de inicialização do sistema;
- Verificação dos Softwares Instalados;
- Otimização do sistema;

Toda manutenção será registrada para documentação e futuras verificações e relatórios.

UTILIZAÇÃO DE REDE

Esse tópico visa definir as normas de utilização da rede que engloba desde o login, manutenção de arquivos no servidor, acesso a Clientes, acesso VPN e tentativas não autorizadas de acesso.

- Não é permitido tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta (também conhecido como "cracking"). Isso inclui acesso a dados não disponíveis para o usuário e/ou conexão a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário;
- Não é permitido interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques do tipo "negativa de acesso", provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de "quebrar" (invadir) um servidor;
- Não é permitido o uso de qualquer tipo de programa ou comando designado a interferir com sessão de usuários;
- Não é permitido o uso de programas P2P e de trocas de arquivos, softwares ou musicas entre a Internet;
- Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas acessados, evitando, desta maneira, o acesso por pessoas não autorizadas e se possível efetuar o logout/logoff da rede ou bloqueio do desktop através de senha. Caso não seja possível o Logoff, o usuário deverá efetuar o bloqueio de sua estação com o comando Crtl Alt Del;

- É necessário que o usuário(a) efetue manutenção no diretório pessoal, evitando acúmulo de arquivos não inerentes à organização;
- Material de natureza pornográfica e/ou racista não poderá ser acessado, exposto, armazenados, distribuídos, editados ou gravados através do uso dos recursos computacionais da rede;
- Não é permitido criar e/ou remover arquivos fora da área destinada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas;
- Cada usuário terá acesso apenas à parte da Rede que tenham informações relacionadas e necessárias ao desenvolvimento de suas atividades.
- Não é permitido o acesso a compartilhamentos não autorizados para seu usuário. Consulte equipe de Infra de quais compartilhamentos estão com acesso autorizado;
- Liberação de acesso a determinadas pastas e compartilhamentos deverão ser solicitadas ao Comitê de Compliance;
- A pasta PÚBLICO ou similar não deverá ser utilizada para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza sensível;
- É obrigatório armazenar os arquivos inerentes à empresa no servidor de arquivos para garantir o backup dos mesmos;
- Arquivos classificados como sigilosos e altamente confidenciais deverão ser armazenados com senha e, preferencialmente criptografados;
- Haverá limpeza semanal dos arquivos armazenados na pasta PÚBLICO ou similar, para que não haja acúmulo desnecessário de arquivos;
- É proibida a instalação ou remoção de softwares que não forem devidamente acompanhadas pelo departamento técnico, através de solicitação escrita que será disponibilizada;
- É vedada a abertura de computadores para qualquer tipo de reparo, os quais serão efetuados exclusivamente pelo departamento técnico Infra;
- Notebooks deverão ser trancados com "cabo de segurança" ou guardados em local seguro, trancados com chave ou entregues para a equipe de Infra/Segurança para guarda em local seguro;
- Não será permitida a alteração das configurações de rede, serviços e inicialização das máquinas bem como modificações que possam trazer algum problema futuro;
- O usuário é obrigado periodicamente a efetuar troca de senha respeitando todas as restrições contidas neste documento;
- O usuário deverá efetuar o backup de seu Outlook frequentemente. Se necessário, o usuário poderá solicitar a equipe de Infra/Segurança a instalação do sistema pfbackup que fará o backup automático dos dados do Outlook;
- Essas regras deverão ser seguidas no acesso Remoto a Rede de Clientes, Fornecedores e outras que façam parte do ambiente organizacional;
- O Acesso Remoto via VPN está limitado somente ao ambiente TS (Remote Desktop), não sendo possível o acesso direto a qualquer outro ambiente da Rede Interna;
- Acessos Remotos via VPN deverão ser autorizados pelo Comitê de Compliance e deverão ser revalidados sempre que necessário pela equipe de Infra;

UTILIZAÇÃO DE E-MAIL

Esse tópico visa definir as normas de utilização de e-mail as quais englobam desde o envio, recebimento até o gerenciamento das contas de e-mail.

- Todos os e-mails trafegados como @EQUITAS.com.br poderão ser monitorados, bloqueados e rejeitados pela empresa, podendo o usuário responder por quaisquer informações trafegadas e "vazadas" através de sua conta. Monitoramento esse respeitando o direito intimidade e ao sigilo das comunicações, nos termos do art. 5, X e XII, da Constituição Federal;
- É restrito o acesso a webmail e caixas postais pessoais dos usuários, podendo a empresa a qualquer momento efetuar o bloqueio/liberação do acesso;
- É proibido o assédio ou perturbação, seja através de linguagem utilizada, frequência ou tamanho das mensagens;
- É proibido o envio de e-mail a qualquer pessoa que não o deseje receber. Se o destinatário solicitar a interrupção de envio e-mails, o usuário deve acatar tal solicitação e não lhe enviar qualquer e-mail;
- É proibido o envio de grande quantidade de mensagens de e-mail ("junkmail" ou "spam") que, de acordo com a capacidade técnica da Rede, seja prejudicial ou gere reclamações de outros usuários. Isso inclui qualquer tipo de mala direta, como, por exemplo, publicidade, comercial ou não, anúncios e informativos, ou propaganda política, correntes e etc.;
- É proibido reenviar ou de qualquer forma propagar mensagens em cadeia ou "pirâmides", independentemente da vontade do destinatário de receber tais mensagens;
- É proibido o envio de e-mail mal-intencionado, tais como "mail bombing" ou sobrecarregar um usuário, site ou servidor com e-mail muito extenso ou numeroso;
- Caso a empresa julgue necessário haverá bloqueios:
    - De e-mail com arquivos anexos que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;
    - De e-mail para destinatários ou domínios que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;
- É proibido forjar qualquer das informações do cabeçalho do remetente;
- É obrigatória a manutenção da caixa de e-mail, evitando acúmulo de e-mails e arquivos inúteis;
- A cota máxima de e-mails armazenados no Servidor não deve ultrapassar os 500 MegaBytes;
- É necessário uso de Pastas Particulares (arquivos PST) para poder efetuar arquivamento dos mails gerenciar caixa postal para não atingir cota máxima de tamanho;
- Obrigatoriedade da utilização do programa Outlook, Mozilla, Webmail Equitas ou outro software homologado pelo departamento técnico, para ser o programa cliente de e-mail;
- Os e-mails e arquivos com informações confidenciais devem ser protegidos. O descarte de e-mails impressos com informação confidencial deve ser efetuado utilizando máquina fragmentadora de papéis e/ou outra forma de descarte seguro.

UTILIZAÇÃO DE ACESSO A INTERNET

Esse tópico visa definir as normas de utilização da Internet que engloba desde a navegação a sites, downloads e uploads de arquivos:

- É proibido utilizar os recursos da empresa para fazer downloads ou distribuição de software ou dados não legalizados;
- É proibida a divulgação de informações confidenciais da empresa em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sujeitando o infrator às penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei;
- Poderá ser utilizada a Internet para atividades não relacionadas com os negócios durante o horário de almoço, ou fora do expediente, desde que dentro das regras de uso definidas nesta política;
- Os funcionários com acesso à Internet podem baixar somente programas ligados diretamente às atividades da empresa e devem providenciar o que for necessário para regularizar a licença e o registro desses programas;
- Funcionários com acesso à Internet não podem efetuar upload de qualquer software licenciado à empresa ou de dados de propriedade da empresa ou de seus clientes, sem expressa autorização do Comitê de Compliance;
- Caso a empresa julgue necessário, haverá bloqueios de acesso à:
    - arquivos que comprometam o uso ou perturbem o bom andamento dos trabalhos;
    - domínios/sites/mail que comprometam o uso ou perturbem o bom andamento dos trabalhos;
    - Restrição completa do acesso Internet de grupos/usuário especificando apenas sites específicos liberados para acesso;
- É expressamente proibido o acesso a sites com conteúdo de Sexo, Bate Papo, Violência, Música, Multimídia, Comunidades, Orkut, Linkedin, Facebook, ou outro qualquer caracterizado como inadequado pela empresa;
- Haverá geração de relatórios dos sites acessados por usuário e se necessário a publicação desse relatório para o Comitê de Compliance;
- Obrigatoriedade da utilização do programa Internet Explorer, Firefox, Chrome ou outro software homologado pelo departamento técnico, para ser o programa cliente de navegação;
- Está liberada apenas a utilização do software de comunicação Skype, desde que dentro das regras de uso definidas nesta política. Não é permitido o uso de outros softwares como ICQ, GoogleTalk, Windows Messenger, MSN, WhatsApp e outros não homologados;
- Conversas dentro de programas de comunicação poderão ser restritas, bloqueadas, e/ou monitoradas, respeitado o direito à intimidade e ao sigilo das comunicações, nos termos do art. 5º, X e XII, da Constituição Federal;
- Não será permitida a utilização de softwares de peer-to-peer (P2P), tais como Kazaa, Emule, Morpheus e afins;
- Não será permitida a utilizarão de serviços de streaming, tais como Rádios On-Line e afins;
- Outros serviços considerados prejudiciais ao desempenho da rede poderão ser bloqueados sem aviso prévio;

UTILIZAÇÃO DE IMPRESSORAS/DOCUMENTOS

Esse tópico visa definir as normas de utilização de impressoras disponíveis na rede interna como manuseio de documentos e informações em papel:

- Ao mandar imprimir, verifique na impressora se o que foi solicitado já está impresso.
    - Se a impressão deu erro e o papel pode ser reaproveitado na sua próxima tentativa, recoloque-o na bandeja de impressão.
    - Se o papel servir para rascunho, leve para sua mesa. Se o papel não servir para mais nada, jogue-o no lixo.
- Não é permitido deixar impressões erradas na mesa das impressoras, na mesa das pessoas próximas a ela e tampouco sobre o gaveteiro;
- Se a impressora emitir alguma folha em branco, recoloque-a na bandeja;
- Se você notar que o papel de alguma das impressoras está no final, faça a gentileza de reabastecê-la. Isso evita que você e outras pessoas tenham seus pedidos de impressão prejudicados e evita acúmulo de trabalhos na fila de impressão;
- Utilize a impressora colorida somente para versão final de trabalhos e não para testes ou rascunhos;
- Somente é permitido o uso de impressoras para fins particulares caso seja autorizado seu uso;
- O usuário da informação deve sempre respeitar o ciclo de vida da informação: geração, uso, transporte, armazenamento e descarte, respeitando e zelando por todo ciclo sua segurança;
- O manuseio e descarte de documentos é de inteira responsabilidade do usuário, devendo o mesmo descartar de forma correta documentos sigilosos e que tenham valor para a organização;

MANUTENÇÃO E CHAMADOS TÉCNICOS

Toda instalação, manutenção (preventiva / corretiva) e suporte referente aos Dispositivos de TI deverão ser efetuados pela equipe de Infra da Equitas respeitando abertura de chamado.

O uso desses Dispositivos de TI quando disponibilizados pela Equitas fora do ambiente de rede deverá ser autorizado pelo Comitê de Compliance respeitando termos destinados, condições e regras aplicados aos mesmos.

Somente será permitido o uso de Dispositivos de TI Pessoais conectados a Infraestrutura de Rede Local se autorizados pela área de Infra e/ou Comitê de Compliance, devidamente documentado e respeitando todas as regras, políticas e procedimentos.

Toda abertura de chamados é de responsabilidade do usuário e deverá ser executada através do e-mail helpdesk@netonze.com.br.

Verificação da utilização de politicas de segurança – testes periódicos

Para garantir as regras mencionadas acima a empresa se reserva o direito de:

- Implantar softwares e sistemas que podem monitorar e gravar todos os usos de Internet através da rede e das estações de trabalho da empresa, respeitado o direito à intimidade e ao sigilo das comunicações, nos termos do art. 5º, X e XII, da Constituição Federal;
- Inspecionar qualquer arquivo armazenado na rede, estejam no disco local da estação ou nas áreas privadas da rede, visando assegurar o rígido cumprimento desta política;
- Efetuar verificações e auditoria pela equipe de Infra/Segurança nos sistemas, estações e rede sem aviso prévio;

A equipe de Infra/Segurança é responsável por testes periódicos e ações preventivas para detectar falhas de segurança e vulnerabilidades. A área de Compliance deve monitorar os resultados desses testes e manter os registros em caso de falhas e violações desta Política.

Nos termos da Política de Segurança, a empresa procederá o bloqueio do acesso ou o cancelamento do usuário caso seja detectado uso em desconformidade com o estabelecido neste documento ou de forma prejudicial à Rede e a Companhia.

Gestão de Vulnerabilidades e Teste de invasão

Gestão de vulnerabilidade é um processo de extrema importância para identificar, categorizar e corrigir as fragilidades nos sistemas, softwares e ambiente tecnológico que suportam a estratégia de negócio da Equitas de acordo com a sua criticidade.

A Equitas realizará anualmente teste de invasão para identificar vulnerabilidades em sistema, softwares e infraestrutura que suporta o negócio da Gestora.

Após a realização da analise de vulnerabilidade, a área de Compliance deverá avaliar o resultado, com objetivo de identificar o risco e plano de ação para mitigação das fragilidades.

Tratamentos de incidentes

Ocorrendo suspeita ou incidente de segurança identificado pelo usuário, o mesmo deverá notificar imediatamente a área de Infra/Segurança a qual fará uma análise completa e levantamento dos sistemas e informações afetadas, assim como a documentação completa do incidente com a notificação ao Comitê de Compliance.

O Comitê de Compliance analisará caso a caso e adotará as medidas cabíveis com base nestes processos:

1.Detecção e Investigação

Todos os incidentes de segurança da informação devem ser classificados (Cód. Malicioso, Phishing, Ransomware, entre outros). Além da categoria do incidente, devem ser levados em conta os seguintes aspectos a fins de triagem e priorização:

- Autor da notificação
- Estado atual do incidente (Se está ocorrendo neste momento)
- Incidente relacionado a um ataque direcionado
- Sistemas afetados
- Sucesso do ataque ou não
- Qualidade das evidências contidas na notificação
- Classificação do incidente (baixo, médio e crítico)

Cada incidente registrado deve ser categorizado e priorizado, conforme sua natureza. Cada incidente deve ter sua causa raiz identificada e documentada, para que sirva de feedback e prevenção/melhoria do ambiente com base em indicadores e lições aprendidas.

Devem ser coletadas informações e evidências das atividades realizadas durante a resposta ao incidente, assim como seus respectivos logs em todas as ferramentas de monitoramento. O produto de qualquer investigação deve ser claro, direto, assertivo e ser baseado em evidências concretas, evitando a possibilidade de haver espaço para conclusões sem análise do ocorrido.

2. Contenção e Erradição

O Comitê de Compliance deverá junto com a área de Infra/Segurança determinar o plano de contenção, correção e erradicação. Proteger os dados confidenciais e sigilosos e em caso de Ransomware, o desligamento das comunicações, restaurando equipamentos/servidores.

3. Recuperação

Após a efetivação contenção, realizar testes para garantir que as vulnerabilidades não continuam em seu ecossistema. Restaurar os recursos remediados. Restaurar dados de backups. Reconstruir sistemas – quando necessário e executar testes finais com o objetivo de garantir a erradicação do incidente.

4. Comunicação

Comunicar formalmente a recuperação do ambiente. Garantir comunicação adequada com as pessoas afetadas e interessadas, inclusive clientes externos.

5. Relatório/Aprendizado

Consolidar e registrar em um único documento se a detecção foi eficiente; verificar se alguma medida ainda não foi adotada e corrigir o processo; verificar se serão necessários novos controles, ferramentas e/ou treinamento adicionais, bem como avaliar o tempo de resposta ao incidente, estimar perdas financeiras, operacionais e reputacionais.

Todo processo deverá ser documentado para análise futura. Em casos de roubo ou vazamento de informações a empresa tomará as medidas legais contra as pessoas envolvidas e punir possível conivência ou falha no cumprimento das exigências estabelecidas na Política de Segurança.

Todas as informações de respeito a incidentes de segurança da informação identificados ou relacionados com a Equitas possuem caráter sigiloso.

Treinamento

A Equitas promove e dissemina a cultura de segurança da informação.

Os colaboradores que tenham acesso a informações confidenciais ou participem de processo de decisão de investimento devem ser treinados a respeito de Segurança da Informação e ameaças cibernéticas. A área de Compliance promove treinamentos de fortalecimento da conscientização da cultura de segurança e prevenção contra ameaças de Phishing, dentre outros.

Termo de Compromisso

Os Colaboradores devem aderir formalmente a um termo, comprometendo-se a agir de acordo com a política de Segurança da Informação.

O Anexo I deste manual contém uma declaração de ciência e adesão a política de segurança descrita que todo colaborador deve preencher e enviar ao Diretor de Compliance assim que houver sua efetivação e devem ser renovados diante de qualquer alteração acordada no Comitê de Compliance.

Das Punições

O não cumprimento pelo usuário, funcionário, parceiro, ou subcontratadas das normas ora estabelecidas neste instrumento (Políticas de Segurança), seja isolada ou cumulativamente, poderá acarretar, de acordo com a infração cometida, as seguintes punições:

- Comunicação de Descumprimento
    - Será encaminhado ao usuário, funcionário, parceiro, ou subcontratado e-mail informando o descumprimento da norma, com a indicação precisa da violação praticada.
    - O Comitê de Compliance será comunicado sobre esse descumprimento.
- Advertência ou Suspensão
    - A pena de advertência ou suspensão será aplicada, por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade.
    -

- Desligamento da Empresa
    - A pena de desligamento da empresa será aplicada a usuário, funcionário, parceiro, ou subcontratado que receba 2 (duas) advertências/suspensões, ou na hipótese de prática de ato de natureza grave.

Disposições e Vigência

As normas descritas não constituem uma relação exaustiva e podem ser atualizadas com o tempo, sendo que modificações serão avisadas em tempo hábil para remodelação (se necessário) do ambiente.

Os participantes do fórum de Segurança da Informação devem manter-se atualizados, discutindo novas vulnerabilidades e ameaças que possam afetar as atividades da Equitas.

A presente política entra em vigor a partir de sua data de publicação até que seja atualizada ou revogada.

ANEXO I – TERMO DE ADESÃO A POLÍTICA DE SEGURANÇA

Eu, _____, portador da Cédula de Identidade número

_____, declaro para os devidos fins que:

1. Tenho total conhecimento da existência da Política de Segurança, a qual recebi, li e comprometo-me a observar integralmente os termos e a acatar e aplicar os princípios contidos na mesma.

2. Sei a partir desta data, que a não observância da Política de Segurança da Equitas poderá implicar na caracterização de falta grave, fato que poderá ser passível da aplicação das penalidades cabíveis, inclusive desligamento por justa causa.

3. As regras estabelecidas da Política de Segurança não invalidam nenhuma disposição do Acordo de Confidencialidade, do Código de Ética nem de qualquer outra regra estabelecida pela Equitas, mas apenas servem de complemento e esclarecem como lidar com determinadas situações na execução das minhas atividades profissionais.

São Paulo, _____de _____ de _____.

_____

Nome: