EQUITAS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Versão 2020.09

Sumário

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 finalidade estabelecer princípios e diretrizes de proteção das informações contra ameaças cibernéticas, considerando a confidencialidade, integridade e disponibilidade para mitigar casos de incidentes de segurança visando minimizar os impactos aos objetivos estratégicos da 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.

Classificação da informação

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

Para informações confidenciais, é necessário um controle de segurança que garanta a proteção dos pilares de segurança da informação (confidencialidade, integridade e disponibilidade). Da mesma forma, informações restritas são de conhecimento reservado em razão de lei, interesse público ou privacidade de dados. Por fim, as informações públicas podem ser divulgadas a qualquer pessoa e empresa, a qual não proporcione impacto ao negócio da Equitas.

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 que guiam as restrições ao uso de sistemas e acessos remotos estão divididas nos seguintes tópicos:

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

É fundamental para a proteção e salvaguarda das informações que os colaboradores adotem comportamento seguro e consistente com o objetivo de proteção das informações da Gestora.

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;
- Sistemas de Antivírus;
- Sistema AntiSpyWare;
- Sistema AntiSpam;
- Atualizações Automáticas – sem interferência humana;
- Manutenção Preventiva;

Para casos específicos relacionados a Phishing, a Equitas, em seu ambiente corporativo, adota as seguintes medidas:

- Ferramentas para proteção ativa contra ameaças digitais – firewall, antivírus, antimalware, antiphishing e antispam;
- Proteções ativas no registro do domínio e servidor de e-mail (SPF/DKIM);
- Habilitação de relatos de ameaças pelos usuários – fornecimento de canal seguro para análise de ameaças recebidas;
- Comunicação – informação periódica sobre ocorrências e formatos recentes de golpes online;
- Educação digital – realização de treinamentos periódicos sobre ameaças digitais e vazamento de informações;

- Validação – realização de testes trimestrais para avaliação da prontidão dos colaboradores e equipe de suporte interno.

Todas as manutenções performadas deverão ser registradas como forma de documentação e como suporte para futuras verificações.

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 pela realização de testes periódicos e ações preventivas para detectar falhas de segurança e vulnerabilidades. Além disso, anualmente, devem ser realizados testes de invasão para detectar vulnerabilidades em sistema, softwares e infraestrutura da Gestora. No caso de detecção de uso em desconformidade com o estabelecido no documento, será realizado o bloqueio de acesso ou cancelamento do usuário.

Tratamentos de incidentes

Em caso de suspeita ou incidente de segurança identificado pelo usuário, a área de Infra/Segurança deve ser notificada imediatamente com o objetivo de realizar uma análise completa e levantamento dos sistemas e informações afetadas. Além disso, a documentação completa do incidente deve ser enviada ao Compliance com o plano de ação adotado, de acordo com as premissas a seguir:

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 (em curso,encerrado...)
- Incidente relacionado a um ataque direcionado
- Sistemas afetados
- Sucesso do ataque
- Qualidade das evidências contidas na notificação
- Classificação do incidente (baixo, médio e crítico)

Cada incidente deverá ser registrado conforme sua natureza categórica e de prioridade. Além disso, cada caso deve ter sua causa raiz identificada e documentada junto as informações e evidências, para que sirva de feedback e prevenção.

2. Contenção e Erradicação

A área de Infra/Segurança de 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 do plano de contenção, realizar testes garantindo que as vulnerabilidades foram superadas.

4. Comunicação

Comunicar, formalmente, a recuperação do ambiente.

5. Relatório/Aprendizado

Consolidar e registrar em um único documento se a detecção foi eficiente. O objetivo da etapa é verificar se alguma medida ainda não foi adotada para a correção do processo, se serão necessários novos controles e/ou ferramentas adicionais e, por fim, avaliar o tempo de resposta ao incidente junto as perdas financeiras, operacionais e/ou reputacionais.

Em casos de roubo ou vazamento de informações a empresa tomará as medidas legais cabíveis

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.

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 um usuário, funcionário, parceiro, ou subcontratado que receba 2 (duas) advertências/suspensões, ou na hipótese de prática de ato de natureza grave.

Plano de Continuidade de Negócio

Com o objetivo de assegurar a continuidade dos negócios em eventos que impliquem na impossibilidade da operação normal em suas instalações principais, a Equitas possui uma série procedimentos para execução do Plano de Continuidade de Negócio ("PCN").

O PCN é desenvolvido para suportar os processos operacionais críticos para a continuidade dos negócios da Equitas e manter a integridade e segurança das execuções de forma que os interesses dos clientes não sejam prejudicados.

Na eventual ocorrência de qualquer evento que impossibilite seu acesso ou permanência nas dependências da Equitas, os Colaboradores devem imediatamente contatar grupo Equitas para orientação quanto à continuidade das atividades fora das dependências da Equitas, bem como se deverão permanecer em suas residências ou dirigir-se a algum local específico durante seu horário normal de trabalho.

Queda de energia

O backup de eletricidade conta com sistema de nobreaks e banco de baterias que visam garantir uma autonomia de até 3 horas de energia, além de outro banco de baterias com autonomia emergencial de mais 2 horas contínuas de uso dependendo da criticidade da função.

Backup e Armazenamento

A Equitas Investimentos possui uma robusta estrutura de TI. Todos os servidores da Equitas são dotados de replicação de HD com redundância de discos (RAID) e Replicação em Site Remoto de Dados e Sistemas de forma Online.

O Servidor de Dados trabalha em clusterização onde na ocorrência de falha de hardware do servidor principal, o servidor secundário assume automaticamente as operações. Diariamente é realizado um Backup de todo o servidor, que é enviado para HD Externo. O HD externo é substituído toda semana com o intuito de garantir uma cópia completa das informações com defasagem máxima de 7 dias fora do escritório.

Queda dos links para acesso à Internet

O escritório possui redundância de Internet com 4 links disponíveis contratados com duas operadoras diferentes (os links são de velocidades 120MB, 100MB, 90MB e 60MB). Os links trabalham em Load Balance, assumindo os serviços de forma automática no caso de falha no link principal.

Contingência para e-mails

O sistema de e-mails possui backups através do sistema Office 365 e possibilita rodarmos o e-mail em servidores da Nuvem da Microsoft.

Contingência serviço de telefonia

A Equitas possui contratados sistemas de telefonia IP via PABX Virtual fornecido pela operadora com garantia de disponibilidade (SLA) de 99,8%. Além disso, para operação de ordens, temos 2 linhas adicionais com outra operadora que podem ser acionadas em caso de indisponibilidade do sistema principal. Todo sistema de telefonia é gravado com retenção de 5 anos.

Equipe Externa

Ainda contamos com um acordo com fornecedor da estrutura de TI que disponibiliza um gerente para solução de eventuais problemas.

Contingências de Computadores ou Situações Extremas

Caso os colaboradores não consigam o acesso físico a Equitas Investimentos, algumas funções possuem uma liberação de contingência remota – via VPN. Dessa maneira o colaborador consegue acesso a rede e a todas as informações essenciais para seguir com as atividades rotineiras. Esse acesso deverá ser feito mediante solicitação e aprovação prévia e estará disponível apenas um acesso Terminal ao computador do usuário.

Testes/Validação

Todos esses processos são vistoriados continuamente visando garantir o bom funcionamento de todo o processo. O Relatório Anual de Monitoramento ainda deve conter recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento.

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 colaboradores 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.

Controle de Versões

Revisão: Set/2020

Próxima Revisão: Set/2021

Revisado por: Giovanna Duarte | Compliance

Aprovado por: Maria Senger | Diretora de Riscos e Compliance
Paulo Lopes | Research - Sócio
Luis Felipe Amaral | Diretor Gestão - Sócio

Histórico de Versões:

202009 Diversos itens alterados referentes a estrutura, redação, monitoramento e controles.

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:

ANEXO II – TERMO DE AUTORIZAÇÃO DE GRAVAÇÕES DE LIGAÇÕES

Eu, _____, portador da Cédula de Identidade nº _____,

declaro para os devidos fins que tenho ciência e autorizo gravar as ligações telefônicas realizadas na Equitas.

São Paulo, _____de _____ de _____.

_____

[Nome completo]

ANEXO III – TERMO DE AUTORIZAÇÃO DE GRAVAÇÕES DE LIGAÇÕES

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 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.

Phishing: Qualquer ataque cibernético que use um e-mail ou mensagem de texto aparentemente válido para induzir o destinatário a acreditar que a comunicação é real e, assim, clicar em um link, fazendo o download de um anexo ou compartilhando diretamente informações pessoais.
Apesar de ser uma técnica de extração de informações bastante antiga, ainda é uma das maneiras mais eficazes de contornar a segurança cibernética de uma pessoa ou empresa, sendo incluída na categoria de engenharia social.

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.

ANEXO IV – SISTEMAS DE SEGURANÇA DE ESTAÇÃO

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.