APUAMA CAPITAL GESTORA DE RECURSOS LTDA.

Política de Segurança da Informação

Janeiro de 2019

Capítulo I
Introdução

Apresentação

1.1. A Apuama Capital Gestão de Recursos Ltda. ("Apuama Capital") é uma sociedade limitada dedicada à prestação de serviço de administração de carteiras de valores mobiliários, notadamente a gestão de fundos de investimento, que consiste no exercício de atividades relacionadas, direta ou indiretamente, ao funcionamento e manutenção destas carteiras.

Objetivo

2.1. A presente Política de Segurança da Informação ("Política") tem por objetivo:

2.1.1. estabelecer diretrizes que permitam aos colaboradores, fornecedores e clientes seguirem padrões de comportamento relacionados à segurança da informação adequados a necessidades de negócio e de proteção legal da empresa e do indivíduo; ·

2.1.2. Desenvolver um Sistema de Gestão da Segurança da Informação que aborde os riscos inerentes ao seu negócio, visando nortear e definir normas e procedimentos específicos de segurança da informação, bem como implementação de controles e processos para seu entendimento;

2.1.3. Preservar as informações da Apuama Capital quanto à:

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

(ii)Confidencialidade: garantia de que o acesso a informação seja obtido somente por pessoas autorizadas

(iii) disponibilidade: garantia de que os usuários autorizados obtenham acesso a informação e aos ativos correspondentes sempre que necessário;

em cumprimento à legislação aplicável, notadamente a Lei nº 9.613, de 3 de março de 1998, alterada pela Lei nº 12.683, de 9 de julho de 2012 ("Lei n° 9.613/98") e a Instrução CVM 301, de 16 de abril de 1999 ("Instrução CVM 301").

2.2. Neste sentido, a companhia pretende, ao instituir a presente Política, estabelecer e implementar procedimentos e controles destinados a:

(I) Política de Segurança da Informação: Descrição e detalhamento do modelo de Segurança da Informação, contemplado a Gestão de Risco; Sistema de Gestão da segurança da Informação-SGSI; e atribuição das responsabilidades e adequação da segurança da informação;

(II) Controles Operacionais de *Hardware*;

(III) Controle de Acesso: Atividade que trata as políticas de controle de acesso aos recursos computacionais (programas,

EQUIPAMENTOS E DADOS), VISANDO A INTEGRIDADE, ACESSIBILIDADE DOS RECURSOS CONTRA ALTERAÇÕES E ATUALIZAÇÕES NÃO AUTORIZADAS, PERDA E DIVULGAÇÃO DE INFORMAÇÕES CONFIDENCIAIS;

(IV) CONTROLE DE ALTERAÇÃO DE *SOFTWARE* APLICATIVOS*:* ATIVIDADE QUE TRATA DO CONTROLE E PREVENÇÃO A QUALQUER TIPO DE ALTERAÇÃO E INSTALAÇÃO DE PROGRAMAS NÃO AUTORIZADOS;

Gestão de Risco

3.1. O processo de Gestão de Risco, visa definir todos os pontos de controle para que se possas realizar uma análise e assim classificá-los e posteriormente estabelecer qual o tratamento adequado para cada caso ou grupo de casos. Essa analise contempla revisões da configuração do sistema e da rede, observação e teste dos controles de segurança implantados. O Risco será reavaliado a cada mudança nas operações da Apuama Capital, ou por influencias externas que afetem suas operações.

3.2. Identificação de Ameaças:

- Humana
  - Humana Involuntária
    - Colaboradores Mal Preparados
    - Distúrbios Urbanos (greves, passeatas etc.)
  - Humana Voluntária
    - Colaboradores Insatisfeitos
    - Crackers, Fraudadores e Insiders
- Não Humana
  - Desastres Naturais
    - Inundações
    - Terremotos
    - Tempestades
  - Falhas Técnicas
    - Hardware
    - Software

- Queda de Energia
- Incêndios e Explosões
- Comunicação e Mídia

3.3. Análise das Vulnerabilidades e Riscos

Classificação	Ameaça	Vulnerabilidade
Humana Involuntária	Colaboradores Mal Preparados	• descarte inadequado de documentos confidenciais • dificuldade de reposição/ cobertura de pessoal qualificado • documentos deixados em fax/copiadora/impressoras • existência de pessoas-chave • falhas na implementação da segurança • falta de comprometimento • falta de treinamento • transmissão de dados confidenciais desprotegidas
Humana Involuntária	Distúrbios Urbanos	• dificuldade de reposição/ cobertura de pessoal qualificado • falhas na implementação da segurança • falta de pessoal
Humana Voluntária	Colaboradores Insatisfeitos	• descarte inadequado de documentos confidenciais • documentos deixados em fax/copiadora/impressoras • estações de trabalho desbloqueadas

		• Estações de trabalho "sabotadas" • Falhas e erros no sistema • Falhas na implementação da segurança • Falta de comprometimento • Política de segurança deficiente • Transmissão de dados confidenciais desprotegidas
Humana Voluntária	Crackers, Fraudadores e Insiders	• Ausência de teste de segurança do ambiente • Configurações inadequadas • Descarte inadequado de documentos confidenciais • Documentos deixados em fax/copiadora/impressoras • Erros de instalação de software • Estações de trabalho desbloqueadas • Falhas na implementação da segurança • Falta de controle no acesso físico • Interrupção dos canais de comunicação • Política de segurança deficiente • Transmissão de dados confidenciais desprotegidas • Uso de software não homologado • Vírus de computadores
Não Humana	Desastres Naturais: Inundação	• Ausência de colaboradores afins treinados • Construção predial inadequadamente dimensionada

		• Falta de recursos para apropriados a inundações
	Desastres Naturais: Tempestades	• Ausência de colaboradores afins treinados • Construção predial inadequadamente dimensionada • Falta de recursos adequados a tempestades
	Desastres Naturais: Terremotos	• Ausência de colaboradores afins treinados • Construção predial inadequadamente dimensionada • Falta de recursos e instalações apropriadas • Falta de recursos para apropriados a inundações
Não Humana	Falhas Técnicas: Hardware	• Falta de qualificação operacional de suporte técnico • Falta de recursos de reserva/ peças sobressalentes • Falhas e erros no sistema • Falhas nos recursos tecnológicos (desgaste, mau uso e obsolescência)
	Falhas Técnicas: Software	• Configurações inadequadas • Cópias não autorizadas/ ilegais • Erros de instalação • Falha na implementação da segurança

		• Falha no ambiente operacional • Falhas e erros no sistema • Falta de treinamento • Política de segurança deficiente • Uso de software não homologado • Acesso irrestrito a documentos eletrônicos
	Falhas Técnicas: Comunicação e Mídia	• Ausência de backup • Configurações inadequadas • Falhas e erros no sistema • Interrupção dos canais de comunicação • Meio de armazenamento com defeito • Radiação magnética afetando a mídia • Transmissão de informações confidenciais desprotegidas
	Falhas Técnicas: Queda de Energia	• Construção predial inadequadamente dimensionada • Falhas de implementação da segurança • Falhas de recursos tecnológicos • Falhas e erros no sistema • Falta de controle de acesso físico • Instalações elétricas inadequadas • Interrupção dos canais de comunicações
	Falhas Técnicas: Incêndios e	• Construção predial inadequadamente dimensionada • Falta de controle de acesso físico

	Explosões	• falta de recursos adequados a explosões • falta de recursos de combate a incêndios • falta de treinamento • instalações elétricas e de gás inadequadas • política de segurança deficiente

3.4. Avaliação das Vulnerabilidades e Riscos

Critérios: Alto risco: 3 Médio risco: 2 Baixo risco: 1 Risco nulo: 0 Vulnerabilidade:	Disponibilidade	Confidencialidade	Integridade	Tratamento do risco	Status
Acesso irrestrito a documentos eletrônicos	3	3	2	Controle de acesso lógico: Uso de software de segurança:	Ok Ok
Ausência de backup	1	2	3	Executar o backup: - Armazenamento na nuvem; - Periodicidade: diária; - Criptografia dos dados;	OK OK OK

				-Restore:	Ok
Ausência de colaboradores afins treinados	2	0	2	Plano de Treinamento.	Implantando
Ausência de teste de segurança do ambiente	3	2	3	Simulação de redirecionamento do ambiente.	Agendado Janeiro / 2019
Configurações inadequadas	2	2	2	Suporte Técnico	Contratado – OK
Construção predial inadequadamente dimensionada	1	1	1	Apropriar a instalação elétrica: Brigada de Incêndio – simulação: Acesso físico: Simulação de contingência.	Nobreak-Ok OK Ok Agendado para Dezembro	2018
Cópias não autorizadas/ ilegais	1	1	3	Política de Homologação de software; Monitoramento da rede; Divulgação da Política de Homologação.	Ok Ok Ok
Descarte inadequado de documentos confidenciais	0	2	2	Fragmentação de documentos (triturar papéis).	Ok
Desmoronamento do edifício	3	0	3	Plano de Recuperação de Desastres.	Ok

Dificuldade de reposição/ cobertura de pessoal qualificado	2	1	2	Plano de Treinamento.	OK
Documentos deixados em fax/copiadora/impressoras	0	2	2	Fragmentação de documentos.	Ok
Erros de instalação de software	2	2	2	Suporte Técnico.	Contratado – OK
Espionagem "industrial"	1	3	2	Controle de acesso físico; Controle de Acesso lógico; Monitoramento e controle da comunicação de dados; Bloqueio de cópias nas estações de trabalho; Propriedade Intelectual.	Ok Ok Ok Ok Ok
Estações de trabalho "sabotadas"	2	2	3	Política de acesso lógico; Monitoramento das estações; Auditoria da Rede; Software de proteção (firewall).	Ok Ok Ok Ok
Estações de trabalho desbloqueadas	3	2	3	Política de acesso lógico; Monitoramento das estações; Auditoria da Rede; Software de proteção	Ok Ok Ok Ok

				(FIREWALL).	
EXISTÊNCIA DE PESSOAS-CHAVE	2	1	2	PLANO DE TREINAMENTO; POLÍTICAS DE RECURSOS HUMANOS.	OK OK
FALHA NO AMBIENTE OPERACIONAL	3	1	3	PLANO DE TREINAMENTO; SIMULAÇÃO DE REDIRECIONAMENTO DO AMBIENTE; SUPORTE TÉCNICO.	IMPLANTANDO AGENDADO JANEIRO / 2019 CONTRATADO – OK
FALHAS DE IMPLEMENTAÇÃO DA SEGURANÇA	2	2	3	REVISAR PERIODICAMENTE A POLÍTICA DE SEGURANÇA; SUPORTE TÉCNICO.	OK - ANUAL | AGENDADO PARA JANEIRO / 2019 CONTRATADO OK
FALHAS E ERROS NO SISTEMA	3	1	3	SUPORTE TÉCNICO; MANUTENÇÃO PREVENTIVA.	CONTRATADO OK OK
FALHAS NOS RECURSOS TECNOLÓGICOS (DESGASTE, MAU USO E OBSOLESCÊNCIA)	3	3	2	SIMULAÇÃO DE REDIRECIONAMENTO DO SISTEMA; SUPORTE TÉCNICO; MANUTENÇÃO PREVENTIVA;	AGENDADO / JANEIRO/ 2019 CONTRATADO OK OK
FALTA DE COMPROMETIMENTO	2	2	2	PESQUISA DE CLIMA ORGANIZACIONAL;	EM ANALISE

				Ações decorrentes ao desdobramento da pesquisa.	Em Analise
Falta de controle no acesso físico	2	2	2	Acesso físico – portaria; Acesso físico – salas.	Ok Ok
Falta de qualificação operacional de suporte técnico	2	1	1	Suporte Técnico.	Contratado
Falta de recursos adequados a explosões	2	0	2	Brigada de Incêndio – simulação;	Agendamento Anual
Falta de recursos de combate a incêndios	2	0	2	Brigada de Incêndio – simulação;	Agendamento Anual
Falta de recursos de reserva/ peças sobressalentes	2	0	1	Equipamentos de Reposição; Inventário dos equipamentos – controle; Suporte Técnico	Ok OK Contratado OK
Fraude e alteração indevida de informações	1	3	2	Monitoramento e controle de pessoal.	Ok
Instalações elétricas e de gás inadequadas	2	0	2	Controle Predial – condomínio; Vistorias periódicas.	Ok Ok
Interrupção dos canais de comunicação	3	1	3	Rota de contingência.	Ok
Meio de armazenamento com defeito	1	1	3	Armazenamento na Nuvem	Ok
Política de segurança	3	3	3	Correção da Política	Ok

Deficiente				de Segurança.	
Proteção contra ferramentas de invasão (sniffer, exploit etc)	3	1	2	Suporte Técnico	Contratado OK
Radiação magnética afetando a mídia	2	0	1	Armazenamento na Nuvem.	Ok
Transmissão de dados confidenciais desprotegidas	1	3	3	Criptografia; Ferramentas de segurança.	Ok Ok
Uso de software não homologado	1	1	2	Política de homologação de software.	Ok
Vírus de computadores	2	2	3	Antivírus (heurístico e de busca); Atualização de antivírus.	Ok Ok

3.5. Tabela de Impacto x Urgência definida pela Diretoria visando demonstrar as prioridades de Ações nas principais atividades pertinentes ao risco:

		Impacto		
		Alto	Médio	baixo
Urgênciaa	Alta	5	4	3
	Média	4	3	2
	Baixa	3	2	1

Impacto = criticidade para o negócio

Urgência = velocidade

3.6. Definição das Prioridades e Pontos de Controle

VULNERABILIDADE	Prioridade	Responsabilidade
Acesso irrestrito a documentos eletrônicos	4	Diretoria
Ausência de backup	3	Diretoria
Ausência de colaboradores afins treinados	4	Diretoria
Ausência de teste de segurança do ambiente	3	Diretoria
Configurações inadequadas	2	Diretoria
Construção predial inadequadamente dimensionada	2	Diretoria
Cópias não autorizadas / ilegais	2	Diretoria
Descarte inadequado de documentos confidenciais	2	Diretoria
Desmoronamento do edifício	1	Diretoria
Dificuldade de reposição/ cobertura de pessoal qualificado	2	Diretoria
Documentos deixados em fax/copiadora/impressoras	3	Diretoria
Erros de instalação de software	2	Diretoria
Espionagem "industrial"	4	Diretoria
Estações de trabalho "sabotadas"	2	Diretoria
Estações de trabalho desbloqueadas	1	Diretoria
Existência de pessoas-chave	3	Diretoria
Falha no ambiente operacional	3	Diretoria
Falhas de implementação da segurança	3	Diretoria
Falhas e erros no sistema	4	Diretoria
Falhas nos recursos tecnológicos (desgaste, mau uso e obsolescência)	2	Diretoria

Falta de comprometimento	2	Diretoria
Falta de controle no acesso físico	2	Diretoria
Falta de qualificação operacional de suporte técnico	4	Diretoria
Falta de recursos adequados a explosões	1	Diretoria
Falta de recursos de combate a incêndios	1	Diretoria
Falta de recursos de reserva/ peças sobressalentes	3	Diretoria
Fraude e alteração indevida de informações	2	Diretoria
Instalações elétricas e de gás inadequadas	3	Diretoria
Interrupção dos canais de comunicação	4	Diretoria
Meio de armazenamento com defeito	2	Diretoria
Política de segurança deficiente	1	Diretoria
Proteção contra ferramentas de invasão (sniffer, exploit etc)	4	Diretoria
Radiação magnética afetando a mídia	3	Diretoria
Transmissão de dados confidenciais desprotegidas	3	Diretoria
Uso de software não homologado	4	Diretoria
Vírus de computadores	2	Diretoria
Acesso irrestrito a documentos eletrônicos	4	Diretoria
Ausência de backup	3	Diretoria
Ausência de colaboradores afins treinados	3	Diretoria
Ausência de teste de segurança do ambiente	2	Diretoria
Configurações inadequadas	3	Diretoria

Sistema de Gestão de Segurança da Informação

4.1. A definição do escopo e os limites dos processos de segurança da informação são orientados pela Diretoria com suporte de empresa contratada, a partir de um estudo e da análise da

avaliação dos riscos, considerando os tratamentos a estes destinados e sua aplicabilidade e impacto ao negócio.

4.2. Responsabilidades e Adequação da Segurança da Informação

4.2.1. Diretoria

(i) Assegurar os recursos necessários para implementação das Políticas de Segurança da Informação

(ii) Garantir o cumprimento das Políticas de Segurança da Informação definidas neste documento

(iii) Promover atualizações periódicas das Políticas de Segurança da Informação

(iv) Aprovar as Ações de Segurança, o Plano de Continuidade de Negócio e Plano de Recuperação e Desastres

(v) Definir e decidir quanto ás medidas a serem tomadas no caso de violação das políticas e as suas sanções, e aplica-las quando de direito.

(vi) Implementar as Ações de Segurança definidas neste documento.

(vii) Garantir que todos os colaboradores estejam cientes das políticas descritas neste documento.

(viii) Elaborar Planos de Ação para implementação das Políticas de Segurança

(ix) Testar a eficácia das medidas da política de segurança da informação

4.2.2. Colaboradores

(I) Estar cientes das Ações de Segurança que lhe compromete

(II)Cumprir as Políticas de Segurança da Apuama Capital.

(III) Comunicar a Diretoria qualquer irregularidade ou desvio de segurança

(IV) Participar das simulações de segurança quando solicitado.

Segurança da Rede de Computadores

5.1. Antivirus: A APUAMA CAPITAL utiliza como software de proteção, para toda sua rede, a solução Bitdefender. – que foi homologado e tem sido atualizado constantemente, a escolha do referido software foi realizada por apresentar monitoramento por técnicas de busca e heurística (para diagnóstico de vírus não catalogados, podendo detectá-los pela variação de determinados arquivos).

5.2. Transmissão de Dados: A transferência de arquivos e dados deve ser protegida com criptografia, para tanto o processamento das cópias de segurança, são protegidos de acordo com o contrato de proteção de dados (DPA) – melhores práticas de privacidade, nas transmissões entre Apuama Capital e Storage - Microsoft.

Política de Segurança Predial

6.1. Análise das Vulnerabilidades

VULNERABILIDADE	PRIORIDADE	RECURSOS
BRIGADA DE INCÊNDIO	2	PREDIAL
BRIGADA DE INCÊNDIO – SIMULAÇÃO	2	PREDIAL
CONSTRUÇÃO PREDIAL MAL DIMENSIONADA	1	PREDIAL
FALTA DE RECURSOS DE COMBATE A INCÊNDIOS	2	PREDIAL

6.3.1 OS PROCEDIMENTOS DE EMERGÊNCIA, A BRIGADA DE INCÊNDIO, CURSOS PREPARATÓRIOS E VISTORIAS SÃO ORGANIZADOS E PERIODICAMENTE TESTADOS PELA ADMINISTRAÇÃO DO CONDOMÍNIO;

6.3.2 A BRIGADA DE INCÊNDIO ESTÁ PREPARADA PARA OS DIVERSOS TIPOS DE INCIDENTES, DESDE O DISPARO DE ALARME, A NECESSIDADE DE EVACUAÇÃO DO EDIFÍCIO ATÉ MOMENTOS DE DESCONTROLE DE PESSOAS. OS EQUIPAMENTOS DE SEGURANÇA COMO EXTINTORES, MANGUEIRAS, ALARMES, LUZES DE EMERGÊNCIA, SENSORES DE FUMAÇA ETC. SÃO VISTORIADOS E REALIZADAS AS MANUTENÇÕES REQUERIDAS, SOB RESPONSABILIDADE DA ÁREA ADMINISTRATIVA;

6.3.3 NÃO EXISTEM PROBLEMAS GRAVES QUANTO AO MAU DIMENSIONAMENTO DAS INSTALAÇÕES FÍSICAS PREDIAIS, INCLUSIVE PERTINENTE AS ROTAS DE FUGA EM CASO DE INCÊNDIO OU SITUAÇÃO QUE REQUEIRA A EVACUAÇÃO DO EDIFÍCIO.

POLÍTICA DE RECURSOS HUMANOS

7.1. ANÁLISE DAS VULNERABILIDADES

VULNERABILIDADE	PRIORIDADE	RECURSOS

Colaboradores cobertura / reposição	2	Rec.Humanos
Comprometimento dos colaboradores	2	Rec.Humanos
Existência de pessoa-chave	3	Rec.Humanos
Pesquisa de Clima Organizacional	1	Rec.Humanos
Treinamento de colaboradores	3	Rec.Humanos

7.2. Comprometimento dos Colaboradores

7.2.1. A contratação de pessoas deve observar a legislação específica e considerar referências de caráter pessoal, profissional e acadêmica.

7.2.2. As responsabilidades por restringir o acesso de funcionários em atividades críticas de operação e programação foram claramente definidas, divulgadas e aplicadas, por meio das Regras e Parâmetros de Atuação.

7.2.3. Os gestores devem ser orientados a observar o comportamento e desempenho dos seus colaboradores, identificando problemas de ordem pessoal que possam comprometer a segurança da organização.

7.2.4. A Diretoria realiza avaliações periódicas do risco, para determinar se as técnicas de controle à segregação de funções estão funcionando como esperado e mantendo o risco em níveis aceitáveis.

7.2.5. A Apuama Capital exige dos funcionários e usuários externos com acesso a informações confidenciais que assinem uma declaração de confidencialidade. Verificando periodicamente as políticas de acordo com confidencialidade juntamente com as Regras e Parâmetros de Atuação.

7.3. Existência de Pessoa Chave: De acordo com a filosofia da Apuama Capital não devem existir colaboradores "proprietários" de informações críticas ou confidenciais, e procura-se realizar trocas de função entre colaboradores com acesso a essas informações periodicamente e as tarefas dos colaboradores são redistribuídas durante suas férias.

7.4. Desligamento de Colaboradores

7.4.1. Os processos de transferência e demissão incluem fluxo de procedimentos de segurança tais como devolução de crachás, chaves e alteração de senha de acesso a email;

7.4.2. Definição do período em que o funcionário afastado ficará sujeito à guarda do sigilo das informações confidenciais às quais teve acesso;

7.4.3. Quando do desligamento de colaboradores, devem ser revogados todos os seus dispositivos de acesso, físico e lógico, e o seu ingresso nas instalações da Empresa deve obedecer aos mesmos critérios definidos para visitantes;

Política de Confidencialidade de Documentos

8.1. Análise das Vulnerabilidades

VULNERABILIDADE	PRIORIDADE	RECURSOS
DESCARTE INADEQUADO DE DOCUMENTOS	2	CORPORATIVO

8.2. O ACORDO DE CONFIDENCIALIDADE É UMA PRÁTICA ASSIMILADA À CULTURA DA ORGANIZAÇÃO ONDE FAZ PARTE DOS PROCEDIMENTOS DE CONTRATAÇÃO, COMPREENDENDO DESDE A ORIENTAÇÃO ATÉ UMA APRESENTAÇÃO PREPARADA PARA ESTA FINALIDADE.

8.3. OS COLABORADORES DA APUAMA CAPITAL SÃO INSTRUÍDOS A REALIZAR A DESTRUIÇÃO DE DOCUMENTOS, QUANDO DE SUA INUTILIZAÇÃO, POR MEIO DO USO DE EQUIPAMENTOS DE TRITURAÇÃO E FRAGMENTAÇÃO DE PAPEL.

8.4. O ACESSO À INFORMAÇÕES SIGILOSAS, FÍSICAS OU DIGITAIS, SÓ PODE SER CONFERIDO PELO DIRETOR DE COMPLIANCE, MEDIANTE SOLICITAÇÃO POR E-MAIL, E SÓ DEVERÁ SER CONFERIDO QUANDO A FUNÇÃO DO COLABORADOR, PARA SEU FIEL CUMPRIMENTO, ASSIM O EXIGIR.

8.4.1. A ÁREA DE *COMPLIANCE* IRÁ MANTER UM CONTROLE EM PLANILHA DE TODOS AS PERMISSÕES CONCEDIDAS, A QUEM FOI FEITA A CONCESSÃO, BEM COMO ÀS INFORMAÇÕES AS QUAIS ELAS SE REFEREM.

8.4.2. NO CASO DE UM COLABORADOR MUDAR DE ÁREA, A ÁREA DE *COMPLIANCE* FICARÁ RESPONSÁVEL POR REVOGAR AS PERMISSÕES CONCEDIDAS, QUANDO CABÍVEL.

8.5. O ACESSO À INFORMAÇÕES SIGILOSAS OU SISTEMAS QUE LIDEM COM ESTAS NÃO SERÁ PERMITIDO DE FORMA REMOTA.

8.6. Em caso de vazamento de informações confidenciais, o evento será imediatamente informado ao Diretor de *Compliance* que, caso haja negligência, poderá sancionar os envolvidos com punições que podem variar desde advertência até o desligamento. Além disto, caso as informações sejam sensíveis para clientes, estes serão informados do ocorrido pelo Diretor de Compliance.

8.7. No primeiro contato de um colaborador, sócio ou diretor com informações confidenciais, ou no mínimo anualmente, será ministrado pela área de compliance um treinamento para lidar com estas, visando assegurar o correto cumprimento do disposto nesta política, no que tange o manuseio de informações confidenciais.

8.8. A fim de proteger as bases de dados com informações sensíveis, a rede e os computadores da empresa são protegidos por *firewall* e anti-vírús, senhas de acesso segregadas por usuário e espelhamento das informações para localidade diversa.

Licenças de Uso de *Software* e Homologação

9.1. Análise das Vulnerabilidades

VULNERABILIDADE	PRIORIDADE	RECURSOS
Cópias não autorizadas/ ilegais	3	Toda rede
Política de Homologação de Software	2	Toda rede

9.2. Licença de Uso de *Software*: Nenhum colaborador à utilização de software sem homologação e o licenciamento de uso. Para tanto, somente a área de TI (Terceirizada) está autorizada na instalação de programas nos computadores da rede, na sua homologação e pela aquisição das licenças de uso, cuja responsabilidade e procedimentos lhe competem.

9.2.1. Os serviços dispostos pela rede corporativa inibem a instalação de softwares por parte dos usuários, sendo para tanto necessário nível de acesso diferenciado, protegido com senha, para executar a instalação de qualquer software em qualquer estação de trabalho ou servidor da rede.

9.3. Homologação de *Software*: Na homologação de software, primeiro é feita a seleção e a análise comparativa entre as soluções do mercado, observando demonstrações e propostas dos fornecedores, juntamente com a área requisitante do software. É escolhida uma área de armazenamento da rede, que não impactará em nenhuma das atividades corporativas, ou até mesmo em uma estação de trabalho fora da rede (*stand alone*), dependendo dos requisitos de recursos do próprio software e do desenvolvedor da solução. Em prazo não inferior a quinze dias são testadas todas as rotinas do aplicativo, pela área fim.

9.3.1. Após o período de testes são considerados os resultados da análise parametrizados e discutidos com a área fim para que se possa tomar a decisão de compra ou sua recusa, se não forem encontradas soluções passionais o processo é revisto procurando

NOVOS FORNECEDORES CONTRAPOSTOS A POSSIBILIDADE DE DESENVOLVIMENTO PRÓPRIO DE SOLUÇÃO.

FALHA DE COMUNICAÇÃO DE DADOS

10.1. ANÁLISE DAS VULNERABILIDADES

VULNERABILIDADE	PRIORIDADE	RECURSOS
FALHA DE COMUNICAÇÃO DE DADOS	4	TELECOM.

10.2. ALTERNATIVAS DE PROCESSAMENTO DE DADOS E TELECOMUNICAÇÃO: PARA A CONTRATAÇÃO E USO DE CANAIS DE COMUNICAÇÃO A APUAMA CAPITAL TOMA OS DEVIDOS CUIDADOS DE ESCOLHA E DIVERSIFICAÇÃO DE FORNECEDORES PARA QUE SUAS OPERAÇÕES NÃO FIQUEM INDISPONÍVEIS EXCLUSIVAMENTE POR UM ÚNICO FORNECEDOR.

FALHAS E CONFIGURAÇÕES DO AMBIENTE

11.1. ANÁLISE DAS VULNERABILIDADES

VULNERABILIDADE	PRIORIDADE	RECURSOS
CONFIGURAÇÕES DO AMBIENTE	3	TODA REDE
FALHA NO AMBIENTE	4	TODA REDE

11.2. CONFIGURAÇÕES DO AMBIENTE: CONFIGURAÇÃO É UM CONJUNTO DE CARACTERÍSTICAS FÍSICAS E FUNCIONAIS DE HARDWARE E SOFTWARE NECESSÁRIAS AO SEU ADEQUADO FUNCIONAMENTO, DEPENDENDO DE CONHECIMENTOS TÉCNICOS ESPECÍFICOS DO AMBIENTE, PARA DIMENSIONAR

adequadamente a interface entre dispositivos e usuários. Para atender estas necessidades a Apuama Capital contrata serviço de terceiro, bem como o suporte técnico.

11.3. Tratamento de Falhas nos Ambientes: O redirecionamento de servidores (por acesso remoto ou não), os backups regulares e os controles de componentes e usuários são as principais ações destinadas a prover soluções inteligentes, preferencialmente sem gerar interrupções e caso ocorram que sejam com menores impactos aos sistemas principais e de apoio.

11.3.1. Para redução de falhas são estabelecidos procedimentos de controle de inventário, manutenções preventivas, suporte técnico (terceirizados) e reposição de dispositivos de primeira necessidade.

11.3.2. Todos os componentes de rede devem ser classificados de acordo com sua criticidade para a continuidade do negócio e preservados quanto às ameaças físicas e ambientais.

11.3.3. As informações que trafegam no ambiente de rede devem ter garantidas a integridade e confidencialidade, em conformidade com sua classificação.

11.3.4. Os ativos de rede só podem ser utilizados após a sua adequação aos padrões de segurança adotados pela Apuama Capital. Os ativos de rede somente devem ser liberados para uso após efetiva homologação.

11.3.5. Na alienação ou reutilização de equipamentos deve ser assegurada a remoção de informações classificadas como confidenciais e restritas.

Planejamento e Planos de Ações da Área de Tecnologia da Informação e Telecomunicações

12.1. Análise das Vulnerabilidades

VULNERABILIDADE	PRIORIDADE	RECURSOS
Plano Diretor de Informática	1	Corporativo
Política de segurança deficiente	3	Corporativo
Revisão da Política de Segurança	4	Corporativo
Serviço de suporte técnico	3	Toda rede
Teste de segurança do ambiente	4	Corporativo
Uso de software não homologado	2	Toda rede

12.2. Política de Segurança e Análise de Conformidades: Análise para verificação do atendimento a qualquer dos requisitos identificados nas normas, baseia-se em evidências objetivas, cujas não-conformidades informam a Diretoria os pontos de controle e as maneiras em que os sistemas de gestão deixaram de atender aos requisitos e pressupõem ações corretivas. Para seu efetivo encaminhamento são necessários os registros destes pontos de controle, sua análise, a correção e disseminação.

12.2.1. Revisão periódica da análise de riscos e dos planos de ações preventivos e corretivos, incluindo a revisão deste documento, descrevem uma orientação às ações, mas não determinam a descrição dos processos passo-a-passo, ou ainda caracteriza normalização técnica a certificação de qualidade.

12.2.2. Avaliação dos procedimentos de controle, verificando a existência dos seguintes os elementos: controle da entrada de dados, autorização física ou eletrônica para os registros de entrada; medidas de segurança para limitar o acesso aos terminais de entrada e validar a inscrição de colaboradores; procedimentos documentados para o tratamento de erros; medidas corretivas para redução de taxas de erro excessivas; integridade dos dados de entrada; do processamento de dados; de sistemas on-line; e de saída de dados.

12.2.3. Uso de softwares não homologados e sem licenças de uso são considerados como não-conformidades as regras e controle de uso de *softwares* pela Apuama Capital, devendo ser tratado como falha, inclusive de segurança.

12.3. Suporte Técnico Terceirizado: Para manter seu quadro funcional, na área de TI e telecomunicações, dimensionado para execução das suas operações, de forma disponível, integra e com desempenho satisfatório, sem onerar com um grande time de colaboradores, a Apuama Capital define como política a terceirização de serviços.

12.3.1. Os critérios de escolha de fornecedores procedem semelhantes às licitações públicas do tipo carta convite, sendo convidadas empresas idôneas, em número não menor a três empresas, provedoras de soluções pertinentes às necessidades e analisadas caso a caso para decidir qual será a prestadora de serviços, podendo haver negociações. Também é realizada análise

CONTRATUAL, NORMALMENTE PREVENDO UM PERÍODO DE AVALIAÇÃO DOS SERVIÇOS.

12.3.2. O ACOMPANHAMENTO DOS PRESTADORES DE SERVIÇOS É DE RESPONSABILIDADE DA DIRETORIA.

12.4. TESTES PERIÓDICOS DE SEGURANÇA: O PLANO DE CONTINGÊNCIA DO NEGÓCIO, OS SISTEMAS DE INFORMAÇÕES E DEMAIS ITENS QUE AGREGAM AS POLÍTICAS DE SEGURANÇA DEVEM SER TESTADOS PERIODICAMENTE, VARIANDO SUA PERIODICIDADE DE ACORDO SUAS CARACTERÍSTICAS.

12.4.1. OS TESTES DEVEM ABRANGER:

- ACESSO A TODOS OS SISTEMAS DESCRITOS COMO ESSENCIAIS NESTE DOCUMENTO.
- EXAMINAR AS POLÍTICAS DE TESTE E OS RELATÓRIOS DA SUA EXECUÇÃO
- OS PLANOS DE CONTINGENCIA E RECUPERAÇÃO DE DESASTRES DEVEM SER ATESTADOS PELO MENOS DUAS VEZES AO ANO E REVISTOS OS ACORDOS RELACIONADOS PROMOVENDO AJUSTES PARA CORRIGIR QUAISQUER DEFICIÊNCIAS CONSTATADAS DURANTE O TESTE, A MATURIDADE DO PROCESSO DEVE SER ATINGIDA APÓS VÁRIAS REALIZAÇÕES, ONDE POR TANTO SE RECOMENDA QUE NOS PRIMEIROS ANOS SEJAM REALIZADOS EM PERIODICIDADE MENOR.
- OS RESULTADOS DOS TESTES DEVEM SER DOCUMENTADOS E GERAR UM RELATÓRIO COM AS "LIÇÕES APRENDIDAS", CONFORME CICLO DO PDCA, SENDO ENCAMINHADO PARA DIRETORIA.

- Os acessos a aplicativos devem ser gerenciados objetivando controle de permissões e rastreamento, de acordo com as definições de perfis de usuários por funcionalidade

12.5. Controle Operacionais do Sistema de Segurança: Todo o acervo de *softwares* e dados mantidos pela Apuama Capital, em conformidade com seu perfil de utilização e especificidades, deve ser passível de recuperação.

12.5.1. A instalação de softwares nos ambientes deve ser formalmente aprovada pela Apuama Capital.

12.5.2. O ambiente operacional deve ser monitorado, registrando as ocorrências que sejam necessárias para contabilização do uso de recursos, recuperação de informações em situações de falhas, auditorias e rastreamento de tentativas de violação.

Backup

13.1. Análise das Vulnerabilidades

VULNERABILIDADE	Prioridade	Recursos
Backup	4	Nuvem
Meio de armazenamento adequado	2	Nuvem
Radiação magnética afetando a mídia	1	Nuvem

Teste de restore	2	Nuvem

13.2. Cópia de segurança de Dados: Cópias de segurança dos arquivos (*BACKUP*) e a documentação dos sistemas são de responsabilidade dos nossos provedores de acesso responsável pelo armazenamento das informações.

13.2.1. A Apuama Capital armazena todos os documentos e e-mails remotamente em um repositório fornecido pela Microsoft (OFFICE 365), que é responsável pela disponibilidade dos documentos.

13.2.2. Todos os documentos ficam armazenados em uma ferramenta de Gestão chamada de Sharepoint, que possui todos os controles de versionamento e lixeira em dois níveis.

13.2.3. Apesar da ferramenta de Gestão de documento ser hospedada remotamente a administração fica sob responsabilidade da Apuama Capital.

Inventário e Controle de Equipamentos de TI

14.1. Análise das Vulnerabilidades

VULNERABILIDADE	Prioridade	Recursos
Inventário dos equipamentos – controle	2	Toda rede

Equipamentos - desgaste e obsolescência	2	Toda rede
Equipamentos e componentes de reserva	1	Toda rede
Manutenção preventiva	2	Toda rede

14.2. A documentação referente à descrição da rede, suas conexões externas, inventário e configuração de seus ativos, deve ser mantida sempre atualizada, preservando os registros históricos, pois pode servir de apoio a recuperação de falhas

14.3. Para o controle de inventário dos equipamentos de TI e telecomunicações, a Apuama Capital o documenta manualmente e o armazena no repositório de documentos onde o mesmo possui controle de versão.

14.4. Estão agregados ao inventário dos equipamentos de TI e telecomunicações a descrição técnica do equipamento, constando informações, tais como: fabricante, origem, documento fiscal, data, valor, condição de aquisição.

14.5. O acompanhamento da vida útil dos equipamentos orienta a gestão na administração dos investimentos financeiros dedicados à sua área, nas atualizações (*UPGRADES*) que possam realizadas, buscando a melhoria do seu desempenho e prolongando o tempo de vida destes. O mesmo se caracteriza em relação à decisão de atualizações de licença de uso de software (*UPDATES*) e nas correções de falhas de programação.

14.6. O controle de desgaste dos equipamentos reduz os riscos de interrupções não programadas por conta de falhas de equipamentos, garantindo uma maior disponibilidade dos sistemas junto aos usuários. Orientando em ações corretivas e preventivas quanto ao desgaste de equipamento e sua obsolescência, considerando a sua depreciação e direcionando equipamentos mais novos para execução de funções mais críticas da Apuama Capital.

14.7 A Apuama Capital mantém pelo menos um notebook preparado para repor algum outro microcomputador que apresente problema, desta maneira substitui o equipamento com problema pela máquina de apoio, enquanto soluciona o problema, com o mínimo de interrupção possível.

14.8. Na aquisição dos equipamentos a Apuama Capital sempre considera a garantia e o suporte técnico, com os melhores prazos oferecidos no mercado, com contrato de até 24 horas de atendimento no suporte técnico destes.

14.9. São realizadas manutenções periódicas de hardware e de software que são programadas e executadas segundo as orientações dos fornecedores, em circunstâncias que minimizem o impacto na operação e na utilização pelos usuários, com a realização dos testes necessários e sua respectiva documentação.

14.9.1. Quando não houver diretriz neste sentido, os equipamentos são revisados anualmente.

Controle das Estações de trabalho

15.1. Análise das Vulnerabilidades

VULNERABILIDADE	PRIORIDADE	RECURSOS
Estações de trabalho "sabotadas"	3	Desktops

15.2. As principais ações para evitar estações de trabalhos sabotadas, ou seja, denegridas por colaboradores intencionalmente, propõem tratar o comportamento dos colaboradores com diversos cuidados como a segregação de funções, a rotatividade funcional, entrevistas, pesquisa de clima, avaliação de desempenho entre outros instrumentos.

15.2.1. A política de segregação de funções e controles de acesso contribui nos controles às estações de trabalho, pois funções distintas são desempenhadas por diferentes colaboradores, que leva a observação dos seguintes pontos de controle:

(I) As atividades devem estar em conformidade com a segregação de funções pretendida;

(II)As descrições das atribuições dos cargos refletem os princípios de segregação de funções. Examinar as descrições para uma amostra de cargos dentro da administração de segurança e no grupo de usuários.

15.3. Controle de Acesso Lógico

VULNERABILIDADE	PRIORIDADE	RECURSOS
Acesso irrestrito a documentos eletrônicos	3	Toda rede

Controle no acesso físico	2	Predial / Servidores
Estações de trabalho desbloqueadas	3	Desktops
Política de acesso lógico	3	Toda rede

15.3.1. O Controle dos Acessos Lógicos, devem ser exclusivamente concedidos por meio do formulário de Controle de Acesso a Sistemas – CAS. Que por sua vez, deve ser revisado pela DIRETORIA

15.4. Diretrizes do Controle e Acessos Físicos e Lógicos

15.4.1. O Controle de Acesso Físico deve controlar e orientar de maneira a disciplinar a movimentação e circulação de pessoas, materiais, equipamentos e veículos.

15.4.2. Todas as ameaças significativas para a segurança física dos recursos mais vulneráveis devem ser identificadas e tratadas, observando também a disposição física dos recursos..

15.4.3. O acesso físico é limitado aos funcionários que precisam rotineiramente dos recursos computacionais, através de vigias, crachás de identificação, chaves e portas de acesso.

15.4.4. Chaves, e outros dispositivos de acesso de reserva (que não estão sendo usados por colaboradores) são mantidos pela Diretoria.

15.4.5. Visitantes e/ou prestadores de serviços são formalmente registrados e acompanhados.

15.4.6. Procedimentos adequados de abandono da área de risco em situações de emergência e de retorno do pessoal após a

NORMALIZAÇÃO DA SITUAÇÃO IMPEDEM O ACESSO DE PESSOAL NÃO AUTORIZADO ÀS ÁREAS CRÍTICAS DURANTE O EVENTO (AMEAÇA DE INCÊNDIO E OUTROS QUE EXIJAM A DESOCUPAÇÃO DO LOCAL).

15.5. Segurança Patrimonial: O PERÍMETRO DE SEGURANÇA DAS INSTALAÇÕES FÍSICAS DA APUAMA CAPITAL DEVE SER DEFINIDO E PROTEGIDO DE ACESSOS NÃO AUTORIZADOS.

15.5.1. OS RECURSOS DE PROCESSAMENTO DE DADOS DEVEM ESTAR ABRIGADOS EM INSTALAÇÕES APROPRIADAS, SENDO O SEU ACESSO RESTRITO A PESSOAS AUTORIZADAS.

15.5.2. A INFRAESTRUTURA E INSUMOS NECESSÁRIOS À CONTINUIDADE DO NEGÓCIO DEVEM SER PROTEGIDOS E TER SUA DISPONIBILIDADE GARANTIDA.

15.5.3. O ACESSO IRRESTRITO AOS DADOS, PERMITE A UMA PESSOA FAZER MUDANÇAS NÃO AUTORIZADAS E INDESEJÁVEIS AO SISTEMA, BEM COMO OBTER INFORMAÇÕES CONTROLADAS.

15.5.4. O ACESSO A PROGRAMAS APLICATIVOS UTILIZADOS PARA PROCESSAR DADOS PERMITE A MODIFICAÇÃO NÃO AUTORIZADA DESSES PROGRAMAS, OU INTRODUÇÃO DE CÓDIGOS DE PROGRAMAÇÃO MAL-INTENCIONADOS, QUE PODERIAM SER UTILIZADOS PARA OBTER ACESSO A ARQUIVOS DE DADOS, RESULTANDO EM SITUAÇÕES INDESEJÁVEIS.

15.5.5. A AUSÊNCIA DE CONTROLES NAS ESTAÇÕES DE TRABALHO OU EM DISPOSITIVOS DE TELECOMUNICAÇÃO PERMITE A ENTRADA NOS SISTEMAS COMPUTACIONAIS, ONDE SE POSSAM OBTER INFORMAÇÕES CONFIDENCIAIS OU DE USO CONTROLADO; SUBSTITUIÇÃO DE DADOS E/OU PROGRAMAS; CAUSAR DANOS OU AINDA COMPARTILHANDO INFORMAÇÕES CONFIDENCIAIS.

15.5.6. Os objetivos de limitação do acesso visam a garantir que:

(i) Os usuários tenham acesso somente aos recursos necessários para executarem suas tarefas;

(ii) O acesso a recursos de alto risco, tais como softwares de segurança, seja limitado a poucos indivíduos;

(iii) Os funcionários estejam impedidos de executar funções incompatíveis ou além da sua responsabilidade.

15.5.7. A implementação de controles de acesso apropriados exige primeiro a determinação do nível e tipo de proteção adequados a cada recurso e a identificação das pessoas que precisam ter acesso a esses recursos. Essas definições devem ser efetuadas pelos responsáveis de cada área.

15.5.8. Considerando como pontos críticos à adequação dos controles de acesso, tem-se:

(i) Classificação dos recursos computacionais de acordo com sua disponibilidade e vulnerabilidade;

(ii) Atualização da lista de usuários autorizados e seu nível de acesso;

(iii) Implantação de controles lógicos e físicos de prevenção ou detecção de acesso não autorizado;

(iv) Supervisão do acesso, investigação de indícios de violação da segurança; e

(v) Adoção das medidas corretivas apropriadas.

15.6. <u>Políticas de Senha:</u> As senhas são:

(i) Únicas para indivíduos específicos, não grupos;

(II) Controladas pelos usuários e não sujeitas a divulgação;

(III) Alteradas periodicamente a cada 45 dias;

(IV) Não são apresentadas na tela durante sua digitação;

(V) São compostas por seis caracteres alfanuméricos, no mínimo, e impedidas de repetição antes de seis trocas pelo menos;

(VI) Existem recomendações quanto ao uso de nomes e palavras facilmente desvendáveis;

(VII) Fornecidas para o primeiro acesso dos colaboradores são imediatamente alteradas;

(VIII) As senhas devem ser individuais, secretas, intransferíveis e ser protegidas com grau de segurança compatível com a informação associada;

15.6.1. Referentes à política de senhas são normativos:

(I) Códigos de identificação e senhas de uso compartilhado pelos funcionários não são permitidos.

(II) Os sistemas não permitem mais que três tentativas de logon com senhas inválidas.

(III) Uma relação do pessoal em atividade, periodicamente atualizada, é usada para verificar automaticamente a lista de usuários autorizados do sistema para remoção da senha de funcionários demitidos ou transferidos.

(IV) Contas de acesso inativas são supervisionadas e removidas quando deixam de ser necessárias.

(V) As seguintes características das senhas devem estar definidas de forma adequada, contendo caracteres permitidos, tamanho, tempo de vida, forma de troca e restrições específicas;

(VI) A distribuição de senhas aos usuários (inicial ou não) deve ser feita de forma segura. A senha inicial, quando gerada pelo sistema, deve ser trocada no primeiro acesso;

(VII) O sistema de controle de acesso deve permite ao colaborador alterar sua senha sempre que desejar.

(VIII) A troca de uma senha bloqueada só deve ser executada após a identificação positiva do usuário.

(IX) A senha digitada não deve ser exibida;

(X) Os colaboradores com outros dispositivos de acesso, tais como códigos e cartões magnéticos têm consciência da necessidade de sua guarda cuidadosa;

(XI) A perda de códigos e cartões magnéticos deve ser imediatamente comunicada aos responsáveis.

15.6.2. Parâmetros das Senhas:

Parâmetros	Rede - Nuvem
Tamanho mínimo da senha	6
Tempo para expiração	45 dias
Tentativas para bloqueio	3
Duração do bloqueio	Pelo Administrador
Histórico de senhas	6
Complexidade Ativada	Sim

15.7. Especificações de Monitoramento ao Controle aos Acessos:

(I) Colaboradores e aplicações que necessitem ter acesso a recursos das entidades da devem ser identificados e autenticados;

(II) O sistema de controle de acesso deve manter as habilitações atualizadas e registros que permitam a contabilização do uso, auditoria e recuperação nas situações de falha;

(III) Nenhum usuário deve ser capaz de obter os direitos de acesso de outro usuário;

(IV) A informação que especifica os direitos de acesso de cada usuário ou aplicação deve ser protegida contra modificações não-autorizadas;

(V) O arquivo de senhas deve ser criptografado e ter o acesso controlado;

(VI) As autorizações devem ser definidas de acordo com a necessidade de condução das tarefas e considerando o que os colaboradores devem ter acesso apenas aos recursos ou sistemas necessários para a condução de tarefas;

15.8. <u>Manutenção de lista atualizada de usuários autorizados e níveis de acesso:</u> As autorizações de acesso são:

(I) Documentadas em formulários padronizados e mantidos em arquivo organizado e aprovados pela Diretoria;

(II) Aprovadas pelo proprietário do recurso computacional;

(III) A diretoria revisa as autorizações de acesso para verificar se continuam necessárias e adequadas.

(IV) As atividades não usuais devem ser investigadas.

(V) As autorizações de acesso temporárias são:

A. Documentadas em formulários padrão e mantidas em arquivo;

B. Aprovadas pela gerência encarregada;

c. Comunicadas de uma forma protegida para o serviço de segurança;

(VI) Antes do compartilhamento de dados ou programas com outras entidades, são formalizados acordos que definem como esses arquivos e programas serão protegidos. Examinar os documentos de autorização de compartilhamento e os acordos de segurança.

* * *