Assunto	Código
Política	POL 26

Atividade

Segurança Cibernética

CONTEÚDO DESTE DOCUMENTO

Este documento determina os critérios relacionados à Segurança Cibernética. É importante ressaltar que o mesmo se aplica a todos colaboradores, prestadores de serviços de TI ou terceiros de TI contratados da Renascença DTVM. *O termo "colaboradores abrange empregados, menores aprendizes, estagiários e administradores da Renascença DTVM Ltda*.

OBJETIVO DA SEGURANÇA CIBERNÉTICA

Disseminar as regras e diretrizes pertinentes à Segurança Cibernética e instituí-las junto aos processos que possuem acesso as informações sensíveis de clientes e parceiros, conforme o determinado pela Diretoria Executiva e instruções vigentes dos Órgãos Reguladores Banco Central e CVM.

A Instituição entende que a segurança cibernética se refere a um conjunto de práticas que protege a informação armazenada nos computadores e aparelhos de computação e transmitida por meio das redes de comunicação, incluindo a internet e telefones celulares.

DIRETRIZES GERAIS - CORPORATIVA

As regras e diretrizes relacionadas ao Controle de Acesso (via Sistema ADROIT – SAS), Segregação de Funções, Classificação dos tipos de informações utilizadas na Instituição, Recursos Humanos (Contratação e Movimentação de Pessoas), Propriedade Intelectual, Segurança Física, Uso dos Recursos de TI, Processo – Mesa Limpa e Tela Limpa, devem ser seguidas de acordo com o determinado e publicado no Instrumento Normativo Política de Segurança da Informação – Corporativa.

PROCESSO DE AUTENTICAÇÃO

As regras relacionadas à configuração de senha são determinadas, pela Área de Tecnologia da Informação – Segurança da Informação, que adota os requisitos mínimos em conformidade com o definido pelo Órgão Regulador.

Os colaboradores, prestadores de serviços de TI ou terceiros contratados de TI são responsáveis pela confidencialidade de suas respectivas senhas, lembrando que as mesmas são individuais e intrasferíveis.

O padrão de configuração está descrito e publicado no Instrumento Normativo Política de Segurança da Informação – Corporativa.

CRIPTOGRAFIA – PROTEÇÃO DE CONTEÚDO

A Instituição utiliza mecanismo (s) de segurança e privacidade que torna (m) determinada (s) comunicação (ões) ininteligível (eis) para quem não tem acesso aos códigos de “tradução” da mensagem.

A (s) chave (s) criptográfica (s) adotada (s), internamente, propõe (m) a proteção de todos os conteúdos transmitidos, evitando a intercepção por parte de cibercriminosos, hackers e espiões, bem como garantem a confidencialidade das mesmas contra-ataques ativos e passivos e, também, a autenticação de origem e destino, característica obrigatória de um protocolo confiável para distribuição de chaves.

PREVENÇÃO E A DETECÇÃO DE INTRUSÃO

O monitoramento do tráfego de rede, identificação de atividades maliciosas e a geração de informações de log sobre estas atividades, bem como o bloqueio e/ou a interrupção das mesmas é realizado pelo “Sistema de Segurança”, que também dispara alerta sobre a atividade detectada.

Visando a segurança ativa na Instituição é utilizado o “Sistema de Segurança” que responde a atividade suspeita, encerrando uma sessão de usuário ou reprogramando o firewall para bloquear o tráfego de rede de uma fonte maliciosa suspeita, bem como para proteger contra softwares maliciosos.

As regras relacionadas ao Firewall de Aplicação – Proxy de Serviços, estão descritas e publicadas internamente no Instrumento Normativo Política de Segurança da Informação – TI.

MECANISMOS DE RASTREABILIDADE

Tendo como processo extremamente importante para o bom funcionamento das operações e negócios, os sistemas utilizados pela Instituição possuem dados e fatos organizados, ou seja, possuem o registro das ações realizadas, bem como dispõem a capacidade de identificar de onde vem cada um dos registros, alertas e problemas de uma determinada área.

Dentre os sistemas críticos da Instituição (relacionados às operações / negócios e indicados no PCN – Plano de Continuidade de Negócios), que possuem o mecanismo de rastreabilidade e que garantem a segurança das informações sensíveis, está o sistema homologado pela B3 “Sistema Integrado de Administração de Corretoras (SINACOR) ”, que controla toda a movimentação do cliente na corretora, as operações de bolsa, conta corrente e custódia de ativos.

MANUTENÇÃO DE CÓPIAS DE SEGURANÇA DOS DADOS E DAS INFORMAÇÕES

A Instituição possui regras definidas para a realização da manutenção de cópias de segurança dos dados e das informações. Os dados são armazenados em fita, por meio de backup diário, guardado em outro local físico. A cópia diária (backup) compõe todos os arquivos de dados do servidor (base de dados, planilhas, textos, entre outros) e as últimas atualizações efetuadas (inclusões, alterações e exclusões de registros).

A regras sobre o tema estão descritas e publicadas no Instrumento Normativo Política de Segurança da Informação – TI – Item Segurança dos Arquivos / Banco de Dados.

CONTROLE DE ACESSO E SEGMENTAÇÃO DA REDE DE COMPUTADORES

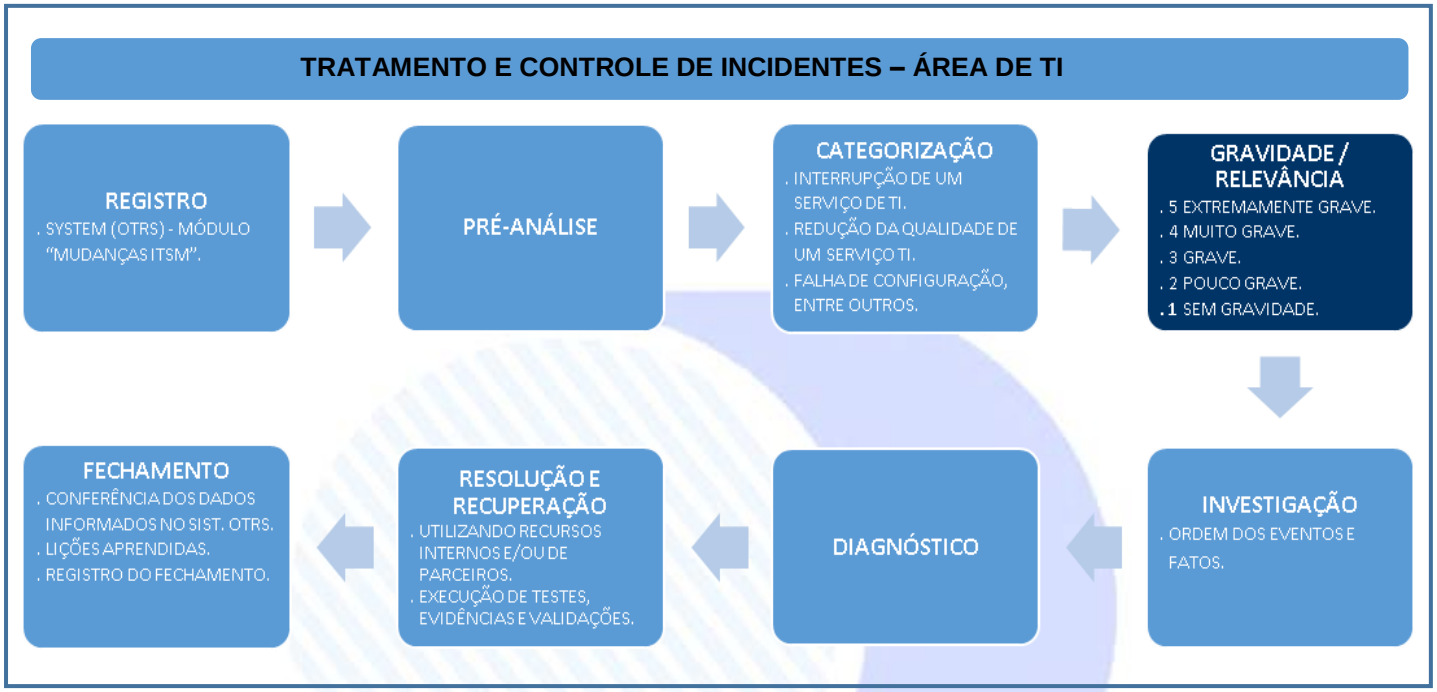
Visando assegurar a integridade do processo de Controle de Acesso - Segregação de Funções, o mesmo foi revisado e implementado, novamente, com novas regras. O processo consiste na separação de atribuições ou responsabilidades entre diferentes colaboradores, especialmente as funções de comercialização, aprovação de operações, controle, contabilização, auditoria e consulta que devem ser apartadas.

As regras e diretrizes estão descritas e publicadas no Instrumento Normativo Política de Segurança da Informação – Corporativa – Item Controle de Acesso e o respectivo detalhamento está publicado no Manual de Controles Internos - Concessão de Acessos aos Sistemas - Segregação de Funções.

FORMALIZAÇÃO E CONTROLES - GESTÃO DE INCIDENTES

Para a Instituição um **incidente de segurança** é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade e os demais **incidentes** (não relacionados à segurança) são eventos que impactam as operações e geram uma interrupção ou diminuição na qualidade do serviço. **Todos os incidentes são registrados por meio de chamado, no Sistema *Open-Source Ticket Request System* (OTRS), onde são definidos os papéis dos envolvidos**.

É importante ressaltar que, os registros, as causas e os planos de ação para o tratamento necessário dos incidentes, também, devem ser descritos no chamado, a qual precisa ser implementada rapidamente para resolver a falha detectada.



Visando a priorização para a resolução de incidentes, devem ser utilizados os critérios estabelecidos na Matriz de Prioridades (modelo abaixo).

Para cada incidente registrado deve ser analisada e definida a respectiva "Priorização / Gravidade", lembrando que situações menos favoráveis recebem nota máxima (5) e as mais favoráveis recebem nota (1). Sendo assim, se o incidente for extremamente grave, urgentíssimo e com altíssima tendência a piorar com o tempo o mesmo deve receber a pontuação conforme a seguir:

Gravidade = 5 | Urgência = 5 | Tendência = 5

NOTA	GRAVIDADE	URGÊNCIA	TENDÊNCIA
5	MUITO ALTA	AGIR IMEDIATAMENTE	AGRAVA RAPIDAMENTE
4	ALTA	AGIR COM URGÊNCIA	AGRAVA EM POUCO TEMPO
3	NORMAL	AGIR O QUANTO ANTES – CURTO PRAZO	AGRAVA NO MÉDIO PRAZO
2	BAIXA	PODE AGUARDAR	AGRAVA NO LONGO PRAZO
1	MUITO BAIXA	SEM PRESSA PARA AÇÃO	NÃO AGRAVA

CUIDADOS DE SEGURANÇA NA COMUNICAÇÃO DE DADOS E VOZ

Por as mesas de operações tratarem diretamente com clientes, as mesmas estão sujeitas à necessidade de validação de termos dos negócios fechados e devem ter suas linhas telefônicas gravadas, visando o registro e o atendimento à exigência regulatória. Os colaboradores envolvidos neste processo, devem estar cientes dessa exigência.

A gravação realizada deve ser arquivada em formato digital pelo prazo mínimo de 05 (cinco) anos. Para mais informações sobre o tema, verificar as regras publicadas na Política Gravação de Voz.

PROTEÇÃO E REVISÃO DE REGISTRO DE EVENTOS (LOGS)

Os sistemas utilitários como gerenciador de banco de dados e outras ferramentas de gestão de rede, especialmente as que acessam dados em Produção, geram o Registro de Operações, é fundamental que os logs gerados sejam protegidos de alteração e deleção. Deve ser realizada a revisão periódica dos mesmos, quer diretamente, quer usando rotina de extração de operações pontuais com software de extração e análise de dados.

Para manuseio, troca e armazenamento de dados não deve ser permitido ao colaborador a extração direta de informações, sem que seja formalizado um pedido, e aprovado pela Diretoria de Operações e/ou Diretoria Administrativa e TI. Para garantir que esta restrição seja efetiva, os dispositivos de leitura e gravação USB são bloqueados. Exceções devem ser deliberadas pela Diretoria Administrativa e TI.

DESCARTE DE MÍDIAS

As mídias de armazenamento permanente ou temporário de informações devem ter tratamento seguro para as situações de descarte, visando proteger a Instituição de exposição não autorizada de informações. Para mais informações sobre o tema, verificar a Política de Segurança da Informação – Corporativa – Item Descarte de Informações.

UTILIZAÇÃO DE EQUIPAMENTOS PERIFÉRICOS

Todos os equipamentos periféricos (que recebem ou enviam informações para o computador, podendo ser, impressoras, mouses, teclados, entre outros) devem ser homologados pela Área de Tecnologia da Informação, sendo necessária a priorização do uso seguro de impressoras e material impresso. No uso cotidiano todos os colaboradores devem adotar a opção de *timeout* nas estações de trabalho, ou seja, ativar a Proteção de Tela do *Windows* protegida por senha, de modo que em ausência maior que 10 minutos, seja ativada esta proteção, salvo exceções mesas e/ou bancadas que possuam terminais de operações.

REDES WIRELESS

A Instituição possui rede sem fio configurada para comodidade e flexibilidade em acessos de natureza específica ou extraordinária. O acesso a rede sem fio somente deve ser permitido mediante aprovação da Diretoria de Operações e/ou Diretoria Administrativa e TI. A rede sem fio da Instituição não permite acesso aos recursos de rede local, sua utilização visa exclusivamente o acesso à internet, de forma irrestrita.
O controle de acesso deve ser efetuado garantindo de forma confiável a restrição de acessos indevidos e/ou maliciosos. O detalhamento deste processo está descrito no Manual de Controles Internos - Concessão de Acessos aos Sistemas - Segregação de Funções.

RELATÓRIO – REGISTRO DE RESPOSTA A INCIDENTES

A Área de Tecnologia da Informação – Segurança da Informação deve preencher o relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31/dezembro. É imprescindível a apresentação do respectivo relatório, à Diretoria Executiva, até 31 de março do ano seguinte ao da data-base.

RESPONSABILIDADES

Diretoria Administrativa e TI

Assegurar que a Política de Segurança Cibernética esteja em conformidade com as regulamentações vigentes e determinação da Diretoria Executiva.

Aprovar a Política de Segurança Cibernética juntamente com Diretor Executivo Administrativo e Financeiro.

Emitir parecer acerca das ações a serem implementadas para correção das deficiências apontadas.

Orientar as áreas e gestores a respeito das regras a serem cumpridas.

Responder aos requerimentos dos Órgãos Reguladores.

Manter esta Política atualizada, juntamente com as áreas de Compliance e Controles Internos e Tecnologia da Informação – Segurança da Informação, devendo o conteúdo ser revisado, no mínimo, anualmente.

Analisar e deliberar o relatório, anual sobre a implementação do plano de ação e de resposta a incidentes, disponibilizado pela Área de Tecnologia da Informação – Segurança da Informação.

Compliance e Controles Internos

Assegurar que as regras estabelecidas nesta Política estejam de acordo com o determinado pela Diretoria Executiva e regulamentações vigentes.

Desenvolver o modelo do relatório anual sobre a implementação do plano de ação e de resposta a incidentes, bem como acompanhar o preenchimento do mesmo pela Área de Tecnologia da Informação – Segurança da Informação.

Fazer com que todos os colaboradores, prestadores de serviços de TI e terceiros contratados de TI tenham conhecimento deste documento.

Diretor Executivo Administrativo e Financeiro

Aprovar a Política de Segurança Cibernética e o relatório anual sobre a implementação do plano de ação e de resposta a incidentes, em consonância com as regulamentações vigentes e diretrizes definidas pela Diretoria Executiva.

Tecnologia da Informação – Segurança da Informação

Executar e manter os procedimentos necessários, garantindo que regras informadas neste documento sejam realizadas, em atendimento às determinações da Diretoria Executiva e Órgãos Reguladores.

Preencher e disponibilizar para aprovação o relatório anual sobre a implementação do plano de ação e de resposta a incidentes.

Colaboradores, Prestadores de Serviços de TI ou Terceiros Contratados de TI da Renascença DTVM

Cumprir integralmente as regras determinadas nesta Política.

Formalizar, junto à Área de Tecnologia da Informação – Segurança da Informação, qualquer ação que não condiz com o determinado nesta Política.

CONFORMIDADE

Lei Anticorrupção

As atividades gerenciais e as operações geradas pela Renascença DTVM são executadas, por seus colaboradores, contratados e administradores, de forma integra e em conformidade com o determinado pelos Órgãos Reguladores e Lei Anticorrupção, qualquer prática contraria é repudiada pela mesma.

Visando preservar a integridade de sua reputação e mantendo o cumprimento à Lei Anticorrupção (Lei nº 12.846/2013), a Renascença DTVM estabeleceu o Manual de Procedimentos Princípios Éticos e Regras de Conduta - AGI 04 e a Política Anticorrupção - POL 09 sendo obrigatório o conhecimento e a aplicação de seus conteúdos por todos os colaboradores, contratados e administradores.

EXCEÇÃO à POLÍTICA DE SEGURANÇA CIBERNÉTICA

Havendo qualquer exceção relacionada às regras e diretrizes estabelecidas nesta Política, a mesma deve ser aprovada, em primeira instância, pela Diretoria Executiva Administrativo Financeiro e pela Diretoria Administrativa e TI.

Ulisses Ricardo Muniz

Diretor Executivo Administrativo Financeiro

Diretoria de Compliance, Riscos e Ouvidoria

Ana Lúcia Alexandre de Sousa

Diretora Administrativa e T.I.