BSM
SUPERVISÃO DE MERCADOS

ROTEIRO DE TESTES DA AUDITORIA OPERACIONAL

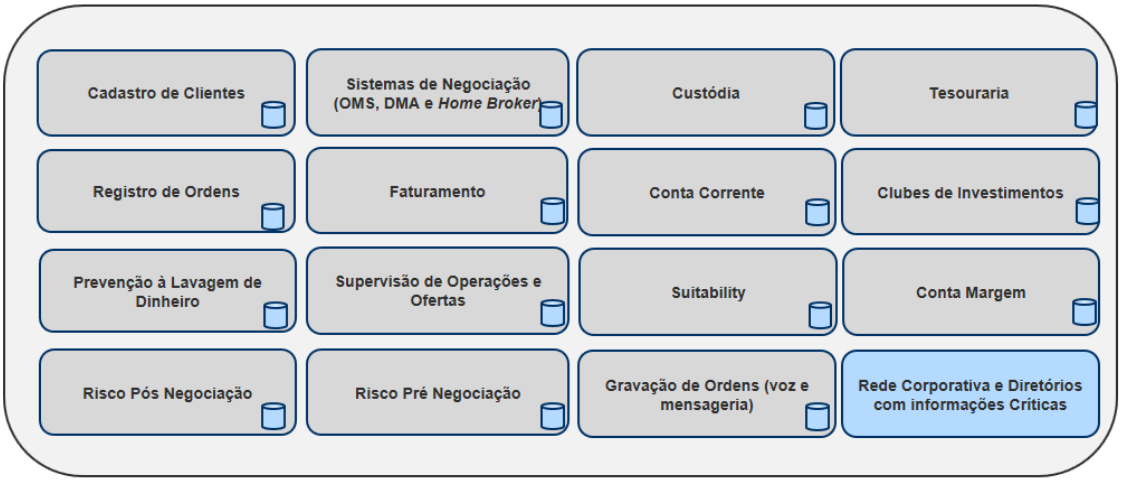
Tecnologia da Informação

Plano de Trabalho 2019

ÍNDICE

PARTICIPANTE DE NEGOCIAÇÃO PLENO e PARTICIPANTE DE NEGOCIAÇÃO

Escopo – Auditoria TI



Período base da auditoria

Para os testes que consideram os 3 meses do período base da auditoria, considerar período conforme tabela abaixo:

Início da Auditoria	Período Base da Auditoria
Janeiro-19	De setembro/2018 a novembro/2018
Fevereiro-19	De outubro/2018 a dezembro/2018
Março-19	De novembro/2018 a janeiro/2019
Abril-19	De dezembro/2018 a fevereiro/2019
Maio-19	De janeiro/2019 a março/2019
Junho-19	De fevereiro/2019 a abril/2019
Julho-19	De março/2019 a maio/2019
Agosto-19	De abril/2019 a junho/2019
Setembro-19	De maio/2019 a julho/2019
Outubro-19	De junho/2019 a agosto/2019
Novembro-19	De julho/2019 a setembro/2019
Dezembro-19	De agosto/2019 a outubro/2019

As principais alterações dos testes em relação ao Roteiro de Testes do Plano de Trabalho de 2018, em decorrência de novos requisitos ou novas abordagens dos testes, estão destacadas em azul.

A. SEGURANÇA DAS INFORMAÇÕES

1) Política de Segurança das Informações (PSI): Avaliação da suficiência, aprovação e divulgação

Principal Requisito Normativo: Itens 129 e 130.1.2 do Roteiro Básico e Resolução CMN 4.658/2018

Documentos utilizados na Execução do Procedimento de Teste:

- Item 1: Lista de colaboradores ativos
- Item 3: Lista de Agentes Autônomos de Investimento
- Item 16: Política, normas, procedimentos e projetos de Segurança da Informação e de Segurança Cibernética.
- Item 17: Aprovação da Política de Segurança da Informação/ Segurança Cibernética
- Item 18: Termo de responsabilidade assinado (ciência da Política) - se aplicável

Procedimento de Teste

1. Política de Segurança da Informação

1.1) Aprovação da PSI pela Alta Administração

Avaliar se a os documentos de política, normas e procedimentos de Segurança da Informação (item 16) foram aprovados pela alta administração do Participante (item 17).

1.2) Avaliação da Suficiência da PSI

Avaliar se a PSI define as diretrizes de “Confidencialidade e integridade da informação”, “Responsabilidade do uso das senhas”, “Utilização de Internet e de correio eletrônico”, “Utilização de software”, “Concessão e administração de acessos a sistemas, base de

dados e redes", "Segurança física dos ambientes de operação e processamento" e "Prevenção, identificação e tratamento de incidentes de Segurança Cibernética". (item 16).

1.3) Divulgação da PSI

Por meio da relação de colaboradores (itens 1 e 3) e tendo como base o processo de divulgação da PSI definido pelo Participante, selecionar amostra e avaliar se os funcionários, estagiários, terceiros e prepostos estão aderentes ao controle que garante a ciência e cumprimento da PSI (item 18).

1.4) Política de Segurança Cibernética (Resolução CMN Nº 4.658)

1.4.1) Aprovação da Política de Segurança Cibernética

Avaliar se a Política de Segurança Cibernética (item 16) foi aprovada pela alta administração do Participante (conselho de administração ou, em sua inexistência, pela diretoria do Participante) (item 17). (Artigos 2º. e 26 da Resolução CMN 4658).

1.4.2) Avaliação do Conteúdo Mínimo

Avaliar a política de Segurança Cibernética do Participante e verificar se contempla no mínimo, os tópicos definidos no Artigo 3º. da Resolução CMN 4658):

a) Objetivos de segurança cibernética da instituição;

b) Procedimentos e os controles adotados para reduzir a vulnerabilidade do Participante a incidentes e atender aos demais objetivos de segurança cibernética, abrangendo no mínimo (Parágrafo 2º. do Artigo 3º. da Resolução BACEN 4658):

- a autenticação,
- a criptografia,
- a prevenção e a detecção de intrusão,
- a prevenção de vazamento de informações,
- a realização periódica de testes e varreduras para detecção de vulnerabilidades,
- a proteção contra softwares maliciosos,
- o estabelecimento de mecanismos de rastreabilidade,

- os controles de acesso e de segmentação da rede de computadores e
- a manutenção de cópias de segurança dos dados e das informações;

c) Controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis;

d) Registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades do Participante;

e) Diretrizes para: “elaboração de cenários de incidentes considerados nos testes de continuidade de negócios”; “definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição”; “classificação dos dados e das informações quanto à relevância”; e “definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes”;

f) Mecanismos para disseminação da cultura de segurança cibernética no Participante, incluindo: a) Programas de capacitação e de avaliação periódica de pessoal; b) Prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros; e c) Comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética;

g) Iniciativas para compartilhamento de informações sobre os incidentes relevantes (mencionados no item d)).

1.4.3) Avaliação e Aprovação do Plano de Ação e de Resposta a Incidentes

Solicitar Plano de ação para implantação da política de Segurança Cibernética (Artigo 6º. da Resolução CMN 4658), aprovado (Item 17) pela alta administração do Participante (conselho de administração ou, em sua inexistência, pela diretoria do Participante), e verificar se contempla:

a) Ações para adequar a estrutura organizacional e operacional do Participante à Política de Segurança Cibernética aprovada;

b) Procedimentos, rotinas, controles e tecnologias que serão utilizados na prevenção e na resposta a incidentes (conforme Política de Segurança Cibernética);

c) Responsável pelo registro e controle de incidentes relevantes.

1.5) Programa de Conscientização

O Participante deve elaborar programa de conscientização e/ou capacitação com treinamentos que envolvam aspectos de segurança cibernética aos colaboradores e prestadores de serviços. Fazem parte desse programa de conscientização os mecanismos para disseminação da cultura de segurança cibernética no Participante, mencionados nos itens 1.2 e 1.4.2 desse roteiro de testes.

1.5.1) Avaliação do Programa de Conscientização

Obter do Participante o Programa de Conscientização de Segurança Cibernética (Políticas e Procedimentos) e avaliar:

a) Abrangência: Avaliar se o programa abrange colaboradores, prepostos e prestadores de serviços;

b) Frequência: Avaliar se o programa possui frequência mínima anual;

c) Aplicação: Avaliar se o programa contempla treinamentos e/ou testes sobre o cumprimento da política de segurança cibernética, de que são exemplos: palestras, *workshop*, teste de *phishing*, quiz.

d) A aplicação de treinamentos por meio phishing (tentativa de adquirir informações disfarçando-se de uma fonte confiável em uma comunicação eletrônica), spam (envio de mensagens não solicitadas em massa) e *e-mails* fraudulentos (mensagens solicitando informações pessoais ou de responsabilidade do Participante) são exemplos de testes para determinar o nível de conscientização, no entanto, devem ser aplicados e geridos de forma controlada pelo Participante para não causar problemas de privacidade em caso de gestão inadequada.

e) Medição da aderência: Avaliar se o programa possui processo para avaliação dos resultados sobre a aderência ao programa aplicado aos colaboradores, prepostos e prestadores de serviços, contendo planos de ação para os resultados obtidos. São exemplos dessa medição: Resultado das provas ou questionários aplicados para medir a conscientização ao final dos treinamentos e plano de ação para colaboradores/prepostos que não atingiram o nível de conscientização mínima esperada.

Como a frequência mínima do programa esperada é anual, e a vigência do requisito é a partir de janeiro de 2019, o Programa de Conscientização poderá ser avaliado pela suficiência do desenho do programa (ainda não aplicado).

2) Processo Monitoramento dos Acessos aos Bancos de Dados

Principais Requisitos Normativos: Itens 130 e 137 do Roteiro Básico

Documentos utilizados na Execução do Procedimento de Teste:

- Item 1: Lista de colaboradores ativos
- Item 10: Lista de usuários de banco de dados
- Item 20: Trilha de auditoria dos bancos de dados
- Item 42: Mapeamento de Infraestrutura de TI

Procedimento de Teste

2.1) Inventário dos Bancos de Dados que Suportam os Sistemas de Escopo

Elaborar documento relacionando (inventário) os bancos de dados dos sistemas aplicativos que suportam os processos de negócios do escopo da auditoria da BSM (Cadastro de Clientes, *Suitability*, Executar Ordens, Liquidar Negócios, Administrar Custódia de Ativos e Posições, Gerenciar Riscos, Clubes de Investimentos, Conta Margem e Supervisão de Operações e Ofertas e Prevenção à Lavagem de Dinheiro). Esses bancos de dados relacionados nesse documento devem constar no Mapeamento da Infraestrutura de TI (item 42).

2.2) Levantamento dos Procedimentos para Monitoração de Acessos Terceiros nos Bancos de Dados

De posse do inventário dos bancos de dados dos sistemas aplicativos que suportam os processos de negócios do escopo da auditoria da BSM (vide etapa 2.1 do Teste de Auditoria), identificar qual desses bancos de dados permitem acessos de terceiros (fornecedores) por meio remoto (acesso via ambiente externo à rede de computadores do Participante) e/ou presencial. Realizar o levantamento dos procedimentos e controles existentes para conceder e monitorar os acessos desses terceiros a esses bancos de dados, contemplando:

a. Quem são os terceiros e em quais bancos de dados e usuários utilizados para acesso;

b. Como e quando esses terceiros realizam os acessos a esses bancos de dados;

c. Quem são os responsáveis pela monitoração (colaboradores / áreas) e para quais bancos de dados; e

d. Como e quando é realizado o monitoramento desses acessos de terceiros nesses bancos de dados – Indicar os controles e ferramentas utilizados para essa monitoração. São exemplos de controles para monitoração: registros das atividades realizadas pelos terceiros nos bancos de dados por meio de gravação de vídeo, trilha de auditoria ou manutenção assistida.

   Prestador de serviço com acesso direto e contínuo ao Banco de dados: Nesse modelo, o prestador de serviço possui acesso contínuo e direto à base de dados, ou seja, pode acessar o banco de dados a qualquer momento sem necessidade de liberação do acesso pelo Participante. Seguem exemplos de procedimentos em conjunto de como acompanhar as atividades realizadas pelo prestador de serviço:

   - O usuário de banco de dados utilizado por prestador de serviço deve ser de conhecimento do Participante.

   - Monitoração das ações por meio da habilitação da trilha de auditoria do banco de dados. A trilha de auditoria pode ser habilitada com filtros de usuários, tabelas e transações com o objetivo de diminuir o impacto na *performance* e reduzir o espaço em disco utilizado pelo banco de dados. A monitoração da atividade de consulta ("*select*") na base de dados também é necessária, pois permite que a base inteira de cliente seja coletada.

   - Análise periódica realizada pelo Participante das trilhas de auditoria referente às atividades executadas diretamente nas bases de dados.

   Prestador de serviço com acesso ao Banco de Dados mediante liberação do Participante: Nesse modelo, o acesso à base de dados é realizado sob demanda, por meio de ferramenta de conexão remota e liberação do Participante. Seguem exemplos de controles:

   - Monitoração das ações por meio da habilitação da trilha de auditoria do banco de dados. A atividade de consulta ("*select*") na base de dados também é necessário monitorar, pois permite que a base inteira de cliente seja coletada.

- Análise periódica realizada pelo Participante das trilhas de auditoria referente às atividades executadas diretamente nas bases de dados.

- Gravação de vídeo ou capturas de tela ("*printscreen*"): gravação da tela com a sessão de conexão ao banco de dados pode ser gravada para evidenciar as ações executadas pelo fornecedor no período de acesso.

- Manutenção assistida: Participante acompanha as atividades realizadas durante o período de acesso.

2.3) Identificação dos acessos de terceiros aos Bancos de Dados

Obter a relação de usuários e permissões de acesso (item 10) aos bancos de dados dos sistemas aplicativos que suportam os processos de negócio do escopo da auditoria da BSM (Cadastro de Clientes, *Suitability*, Executar Ordens, Liquidar Negócios, Administrar Custódia de Ativos e Posições, Gerenciar Riscos, Clubes de Investimentos, Conta Margem e Supervisão de Operações e Ofertas e Prevenção à Lavagem de Dinheiro).

De posse do levantamento dos procedimentos para monitoração dos acessos de terceiros nos bancos de dados (vide etapa 2.2 do Procedimento de Teste de Auditoria) e da lista de colaboradores ativos (terceiros) (item 1), identificar na relação de usuários e permissões de acessos nesses bancos de dados os usuários utilizados por esses terceiros.

2.4) Avaliação da Monitoração dos Acessos de terceiros aos Bancos de Dados

Com base no levantamento dos procedimentos para monitoração dos acessos de terceiros nos bancos de dados (vide etapa 2.2 do Procedimento de Teste), obter os registros das atividades realizadas do controle / ferramenta identificado nesse levantamento (são exemplos de controles para monitoração: registros das atividades realizadas pelos terceiros nos bancos de dados por meio de gravação de vídeo, trilha de auditoria ou manutenção assistida), no período de 1 mês (item 20). De posse desses registros de atividades, avaliar se permitem identificar o usuário, data, horário e evento de efetuado no banco de dados (alteração, inclusão ou exclusão).

3) Parâmetros de Senha e de Segurança

Principais Requisitos Normativos: Itens 130.1.1, 131, 132 e 135 do Roteiro Básico

Documentos utilizados na Execução do Procedimento de Teste:

- Item 13: Planilha de sistemas de negociação
- Item 22: Parâmetros de segurança de senha da rede corporativa e sistemas escopo
- Item 23: Parâmetros de segurança de senha de clientes nos canais de relacionamento eletrônico
- Item 24: Evidência de certificado digital do canal de relacionamento
- Item 25: Evidência de criptografia no tráfego de informações críticas
- Item 26: Evidência do duplo fator de autenticação
- Item 27: Trilhas de auditoria dos registros de entrada/saída dos Canais de relacionamento eletrônico com os clientes
- Item 28: Evidência de troca de senha no primeiro acesso do cliente
- Item 29: Planilha de sistemas

Procedimento de Teste

3.1) Inventário dos sistemas escopo de análise

Inventariar os sistemas aplicativos e de negociação que suportam os processos de negócio relacionados à auditoria da BSM e os canais de relacionamento eletrônico oferecidos pelo Participante aos seus clientes (itens 13 e 29).

3.2) Parâmetros de senhas: sistemas internos e utilizados por clientes

Acessos de sistemas internos e de clientes possuem diferentes requisitos de parâmetros de senha e a análise da aplicabilidade de cada parâmetro deve ser avaliada conforme tabela a seguir:

Tipo de acesso (Item do RB)	Tamanho Mínimo	Tempo de Expiração	Tentativas para Bloqueio	Duração do Bloqueio	Histórico	Complexidade	Criptografia	Dupla Autenticação	Troca de senha no primeiro acesso
Internos (RB 131) (A)	6 caracteres	90 dias	5 tentativas	Desbloqueio mediante avaliação do Administrador	6 senhas	Ativada	Ativada	*Não Requerido*	**(E)**
Clientes - DMA (RB 132) (B)	6 caracteres	*Não Requerido*	5 tentativas	Desbloqueio mediante confirmação da identidade **(D)**	*Não Requerido*	*Não Requerido*	Ativada	*Não Requerido*	Sim
Clientes - *Canais* (RB 135) (C)	6 caracteres	*Não Requerido*	5 tentativas	Desbloqueio mediante confirmação da identidade **(D)**	*Não Requerido*	*Não Requerido*	Ativada	Sim **(F)**	Sim

(A) A avaliação dos requisitos de parâmetros de senhas para os sistemas internos abrange os acessos à rede de computadores, sistemas aplicativos, sistemas eletrônicos de negociação e canais de recebimento de ordens de clientes, inclusive ordens recebidas por aplicativo de celular.

(B) A avaliação dos requisitos de parâmetros de senhas para acessos de clientes nos sistemas eletrônicos de negociação abrange as ferramentas fornecidas e gerenciadas pelo Participante ou por terceiros por ele contratado. Não serão avaliados os requisitos de parâmetros de senhas de sistemas eletrônicos de negociação contratados pelo próprio cliente (a contratação e/ou desenvolvimento do sistema é do próprio cliente, sem gestão do Participante).

(C) A avaliação dos requisitos de parâmetros de senhas abrange os canais de relacionamento eletrônico do Participante (*site* da internet disponibilizado pelo Participante para consulta e transações de clientes).

(D) Senha bloqueada só pode ser desbloqueada mediante confirmação da identidade do usuário pelo Participante (confirmação de dados pessoais, cadastrais e/ou de operações).

(E) Troca da senha padrão fornecida pelo fabricante do sistema operacional, do software de terceiros ou de sistemas.

(F) Aplicável apenas para transações (de que são exemplos: negociação, atualização cadastral, preenchimento de questionário de suitability, transferência de custódia), não é obrigatório para consulta de informações.

3.3) Avaliação dos parâmetros de senha e de segurança das informações

A averiguação dos parâmetros de senha pode ser realizada por meio da análise de telas de configuração de parâmetros de senha, trilhas de auditoria e por meio de simulação. Faz parte dos procedimentos da auditoria, avaliar *in loco* , por meio de simulação, parte dos parâmetros recebidos em telas de configuração ou trilhas de auditoria.

3.3.1) Tamanho mínimo da senha

Este parâmetro de senha é aplicável para os seguintes tipos de acesso: Internos, Clientes – DMA e Clientes – Canais.

a) Procedimento de teste por meio de tela de configuração de parâmetros de senha

De posse da tela de configuração de parâmetros de senha (itens 22 e 23), verificar se o parâmetro Tamanho Mínimo possui o valor de 6 caracteres ou superior.

b) Procedimento de teste por meio simulação de comportamento

De posse de um usuário do sistema criado para testes em comum acordo com o Participante e que deve ser removido após a simulação de parâmetros, efetuar o cadastro de uma nova senha, contendo de 1 a 5 caracteres. Exemplo: “A”, “abc”, “1234a”, etc.

Se não for permitido o cadastro da senha com o tamanho inferior a 6 caracteres, o parâmetro Tamanho Mínimo da Senha atende ao requisito.

Se for permitido o cadastro da senha com o tamanho inferior a 6 caracteres, o parâmetro Tamanho Mínimo da Senha não atende ao requisito.

3.3.2) Tempo de expiração da senha

Este parâmetro de senha é aplicável para o seguinte tipo de acesso: Internos.

a) Procedimento de teste por meio de tela de configuração de parâmetros de senha

De posse da tela de configuração de parâmetros de senha (item 22), verificar se o parâmetro Tempo de Expiração possui o valor de 90 dias ou inferior.

3.3.3) Quantidade máxima de tentativas de acerto de senha antes do bloqueio (Tentativas Bloqueio)

Este parâmetro de senha é aplicável para os seguintes tipos de acesso: Internos, Clientes – DMA e Clientes – Canais.

a) Procedimento de teste por meio de tela de configuração de parâmetros de senha

De posse da tela de configuração de parâmetros de senha (itens 22 e 23), verificar se o parâmetro Tentativas Bloqueio possui o valor de 5 caracteres ou inferior.

b) Procedimento de teste por meio simulação de comportamento

De posse de um usuário do sistema criado para testes em comum acordo com o Participante e que deve ser removido após a simulação de parâmetros, efetuar a tentativa de bloqueio da senha de um usuário com acesso ao sistema, por meio da utilização de senhas incorretas.

Evidenciar as tentativas realizadas e os alertas emitidos pelo sistema até a identificação do bloqueio do usuário, conforme exemplos abaixo:

I – Exemplo de alertas emitidos pelo sistema – parâmetro correto:

1º tentativa: “Senha incorreta. Você possui mais 4 tentativas”.
2º tentativa: “Senha incorreta. Você possui mais 3 tentativas”.
3º tentativa: “Senha incorreta. Você possui mais 2 tentativas”.
4º tentativa: “Senha incorreta. Você possui mais 1 tentativas”.
5º tentativa: “Senha Bloqueada”.

Solicitar ao usuário que efetue o acesso utilizando a senha correta a partir da 6º tentativa. Tendo como base que a configuração está correta, o resultado deve gerar um novo alerta de “Senha Bloqueada”.

II – Exemplo de alertas emitidos pelos sistemas – parâmetro incorreto:

1º tentativa: “Senha incorreta”.
2º tentativa: “Senha incorreta”.
3º tentativa: “Senha incorreta”.
4º tentativa: “Senha incorreta”.
5º tentativa: “Senha incorreta”.

Solicitar ao usuário que efetue o acesso utilizando a senha correta a partir da 6º tentativa. Tendo como base que a configuração está incorreta, como resultado da 6º tentativa, o acesso deve ser permitido, não efetivando o bloqueio.

3.3.4) Duração do Bloqueio da Senha

Este parâmetro de senha é aplicável para os seguintes tipos de acesso: Internos, Clientes – DMA e Clientes – Canais.

a) Procedimento de teste por meio de tela de configuração de parâmetros de senha

De posse da tela de configuração de parâmetros de senha (itens 22 e 23), verificar se o parâmetro Bloqueio da Senha é “Desbloqueio pelo Administrador” para acessos do tipo interno ou “Mediante confirmação da identidade” para acessos de clientes.

b) Procedimento de teste por meio simulação de comportamento

- Duração do bloqueio (Desbloqueio pelo Administrador) (Acessos Internos)

  De posse de um usuário do sistema criado para testes em comum acordo com o Participante e que deve ser removido após a simulação de parâmetros, efetuar o bloqueio do seu acesso ao sistema, por meio da utilização de senhas incorretas e avaliar o procedimento de desbloqueio. O desbloqueio deve ser efetuado somente após a avaliação do administrador do sistema.

- Desbloqueio de senha mediante confirmação da identidade do usuário (Clientes – DMA e Clientes – Canais)

  De posse de um usuário do sistema criado para testes em comum acordo com o Participante e que deve ser removido após a simulação de parâmetros, efetuar o bloqueio do seu acesso ao sistema, por meio da utilização de senhas incorretas e avaliar o procedimento de desbloqueio. O desbloqueio deve ser efetuado somente após a confirmação de informações contidas na ficha cadastral do cliente.

3.3.5) Histórico de Utilização de Senha

Este parâmetro de senha é aplicável para o seguinte tipo de acesso: Internos.

a) Procedimento de teste por meio de tela de configuração de parâmetros de senha

De posse da tela de configuração de parâmetros de senha (item 22), verificar se o parâmetro Histórico possui o valor de 6 senhas ou superior.

b) Procedimento de teste por meio simulação de comportamento

De posse de um usuário do sistema criado para testes em comum acordo com o Participante e que deve ser removido após a simulação de parâmetros, alterar a senha de acesso, no mínimo, 6 (seis) vezes.

Evidenciar as 6 (seis) alterações realizadas e reutilizar a primeira senha de teste, com o intuito de avaliar o bloqueio do sistema, conforme exemplos abaixo:

I – Histórico mínimo de senhas – parâmetro correto:

1º registro de senha: “Teste@1” – Mensagem: “Senha alterada com sucesso. ”
2º registro de senha: “Teste@2” – Mensagem: “Senha alterada com sucesso. ”
3º registro de senha: “Teste@3” – Mensagem: “Senha alterada com sucesso. ”
4º registro de senha: “Teste@4” – Mensagem: “Senha alterada com sucesso. ”
5º registro de senha: “Teste@5” – Mensagem: “Senha alterada com sucesso. ”
6º registro de senha: “Teste@6” – Mensagem: “Senha alterada com sucesso. ”

Solicitar ao usuário que registre a senha pela 7º vez utilizando o valor da primeira senha (“Teste@1”). Tendo como base que a configuração está correta, como resultado do 7º registro de alteração da senha, o sistema não deve permitir a reutilização da primeira senha e emitir um alerta ao usuário. Exemplos: “Senha utilizada recentemente. ”, “Não é permitido reutilizar as últimas 6 senhas. ”, etc.

II – Histórico mínimo de senhas – parâmetro incorreto:

1º registro de senha: “Teste@1” – Mensagem: “Senha alterada com sucesso. ”
2º registro de senha: “Teste@2” – Mensagem: “Senha alterada com sucesso. ”
3º registro de senha: “Teste@3” – Mensagem: “Senha alterada com sucesso. ”
4º registro de senha: “Teste@4” – Mensagem: “Senha alterada com sucesso. ”
5º registro de senha: “Teste@5” – Mensagem: “Senha alterada com sucesso. ”
6º registro de senha: “Teste@6” – Mensagem: “Senha alterada com sucesso. ”

Solicitar ao usuário que registre a senha pela 7º vez utilizando o valor da primeira senha (“Teste@1”). Tendo como base que a configuração está incorreta, como resultado do 7º registro de alteração da senha, o sistema deve permitir a reutilização da primeira senha e emitir um alerta de confirmação da alteração. Exemplo: “Senha alterada com sucesso”.

3.3.6) Complexidade de Senha

Este parâmetro de senha é aplicável para os seguintes tipos de acesso: Internos.

a) Procedimento de teste por meio de tela de configuração de parâmetros de senha

De posse da tela de configuração de parâmetros de senha (item 22), verificar se o parâmetro Complexidade de Senha possui o valor “ativada”.

b) Procedimento de teste por meio simulação de comportamento

De posse de um usuário do sistema criado para testes em comum acordo com o Participante e que deve ser removido após a simulação de parâmetros, alterar a senha de acesso.

Evidenciar as tentativas de alteração de senha, de acordo com os procedimentos abaixo:

- Solicitar ao usuário que registre uma nova senha, respeitando o tamanho mínimo de 6 caracteres, contendo somente letras minúsculas (exemplo: “abcdef”). Tendo como base que a configuração está correta, como resultado o sistema não deve permitir o registro da nova senha.

- Solicitar ao usuário que registre uma nova senha, respeitando o tamanho mínimo de 6 caracteres, contendo somente letras maiúsculas (exemplo: “ABCDEF”). Tendo como base que a configuração está correta, como resultado o sistema não deve permitir o registro da nova senha.

- Solicitar ao usuário que registre uma nova senha, respeitando o tamanho mínimo de 6 caracteres, contendo somente números (exemplo: “123456”). Tendo como base que a configuração está correta, como resultado o sistema não deve permitir o registro da nova senha.

- Solicitar ao usuário que registre uma nova senha, respeitando o tamanho mínimo de 6 caracteres, contendo somente letras maiúsculas e minúsculas (exemplo: “ABCdef”). Tendo como base que a configuração está correta, como resultado o sistema não deve permitir o registro da nova senha.

- Solicitar ao usuário que registre uma nova senha, respeitando o tamanho mínimo de 6 caracteres, contendo letras maiúscula e minúsculas e números (exemplo: “Abc123”). Tendo como base que a configuração está correta, como resultado o sistema deve permitir o registro da nova senha.

3.3.7) Criptografia de Senha

Este parâmetro de senha é aplicável para os seguintes tipos de acesso: Internos, Clientes – DMA e Clientes – Canais.

a) Procedimento de teste por meio de tela de configuração de parâmetros de senha

De posse da tela de configuração de parâmetros de senha (itens 22 e 23), verificar se o parâmetro Criptografia de Senha possui o valor “Ativada”.

b) Procedimento de teste por meio simulação de comportamento

Com acompanhamento da auditoria, solicitar a uma analista DBA com acesso à base de dados do sistema escopo avaliado, que comprove a criptografia da senha de acesso registrada pelo usuário.

A análise da criptografia das senhas deve ser demostrada visualmente ao auditor presente, sem coleta de evidências com dados de usuários e senhas (mesmo que criptografadas).

Para situações em que a criptografia de senha é disponibilizada pelo fornecedor ao Participante, por e-mail, a análise da criptografia das senhas deve ser demostrada da mesma forma, visualmente ao auditor presente, sem a obtenção da evidência.

3.3.8) Dupla Autenticação

Este parâmetro de senha é aplicável para canais de relacionamento eletrônico do Participante para transações (de que são exemplos: negociação, atualização cadastral, preenchimento de questionário de suitability, transferência de custódia), não é obrigatório para consulta de informações.

a) Procedimento de teste por meio de tela de configuração de parâmetros de senha

De posse da tela de configuração de parâmetros de senha (item 26), verificar se o parâmetro Dupla Autenticação de Senha possui o valor “Ativada”.

b) Procedimento de teste por meio simulação de comportamento

De posse de um usuário do sistema criado para testes em comum acordo com o Participante e que deve ser removido após a simulação de parâmetros efetuar o acesso ao sistema para realizar uma transação e avaliar a existência de mais de um fator de autenticação.

Evidenciar o passo a passo de acesso ao sistema, de acordo com os procedimentos abaixo:

I – Solicitar ao usuário que efetue o acesso ao sistema avaliado e, tendo como base que os parâmetros estão corretos, o sistema deve solicitar ao usuário um segundo fator de autenticação, de acordo com os exemplos abaixo:

Autenticação de usuário e senha + Token OTP (senha de utilização única);
Autenticação de usuário e senha + Mensagem de texto (SMS);
Autenticação de usuário e senha + Certificado digital (e-CPF ou e-CNPJ);
Autenticação de usuário e senha + Cartão de senhas.

II – Solicitar ao usuário que efetue uma transação no sistema avaliado e, tendo como base que os parâmetros estão incorretos, o sistema não deve solicitar ao usuário um segundo fator de autenticação e liberar o acesso ao sistema.

III – Solicitar ao usuário que efetue uma transação no sistema avaliado inserindo a mesma senha para a primeira e para a segunda autenticação, tendo como base que os parâmetros estão corretos, o sistema não deve liberar o acesso ao sistema.

3.3.9) Troca de Senha no Primeiro Acesso

Este parâmetro de senha é aplicável para os seguintes tipos de acesso: Clientes DMA e Clientes – Canais.

a) Procedimento de teste por meio simulação de comportamento

De posse de um usuário administrador do sistema, realizar a criação de um login de acesso e geração da senha de acesso inicial do login;

- Evidenciar o recebimento das informações de acesso (usuário e senha padrão) pelo cliente, conforme cadastro realizado no passo anterior;

- Evidenciar o acesso do cliente com as informações recebidas pelo administrador do sistema e avaliar se ao realizar o acesso pela primeira vez o sistema solicita a troca da senha padrão fornecida pelo administrador (item 28).

3.3.10) Certificado Digital e Criptografia no tráfego de informações sensíveis

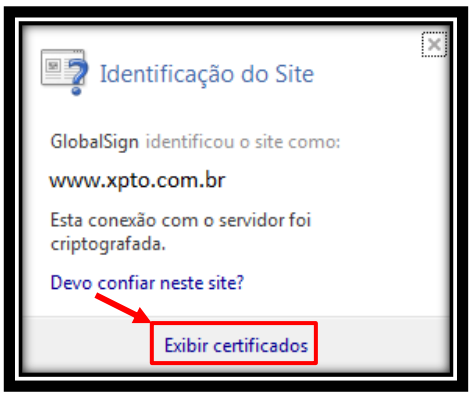
Este parâmetro de senha é aplicável para os seguintes tipos de acesso: Clientes – Canais. Os procedimentos abaixo, utilizados como exemplos, são aplicáveis em ambiente Windows – Internet Explorer.

a) Procedimento de teste por meio simulação de comportamento.

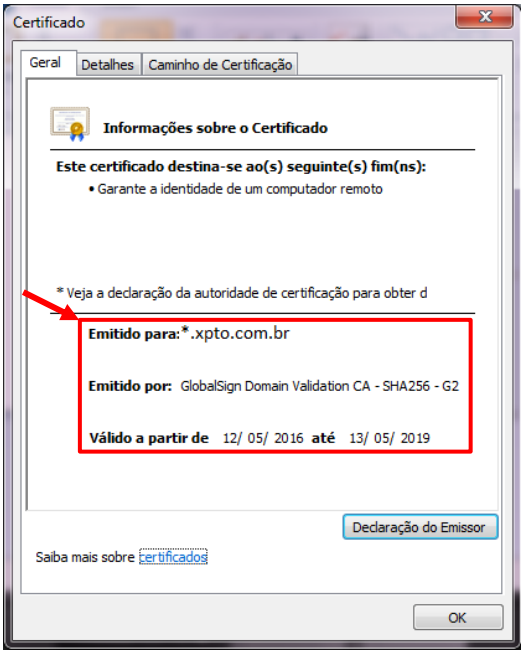
Abrir o canal de relacionamento eletrônico disponibilizado pelo Participante aos seus clientes e realizar os seguintes passos (**itens 24 e 25**):

- Clicar sobre o cadeado disponível no caminho do browser:

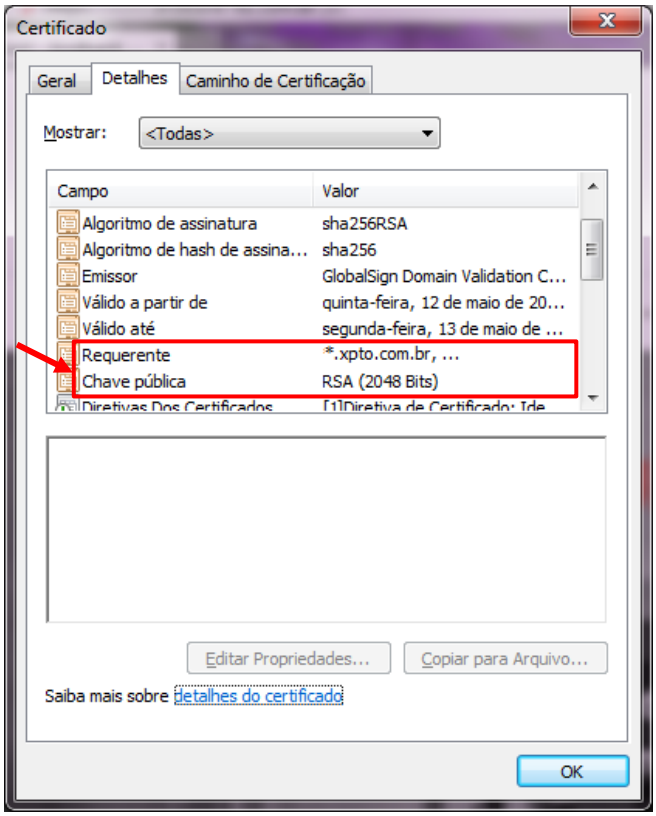
- Após clicar sobre o cadeado, o browser disponibilizará a identificação do site. Clicar em “Exibir Certificados”:



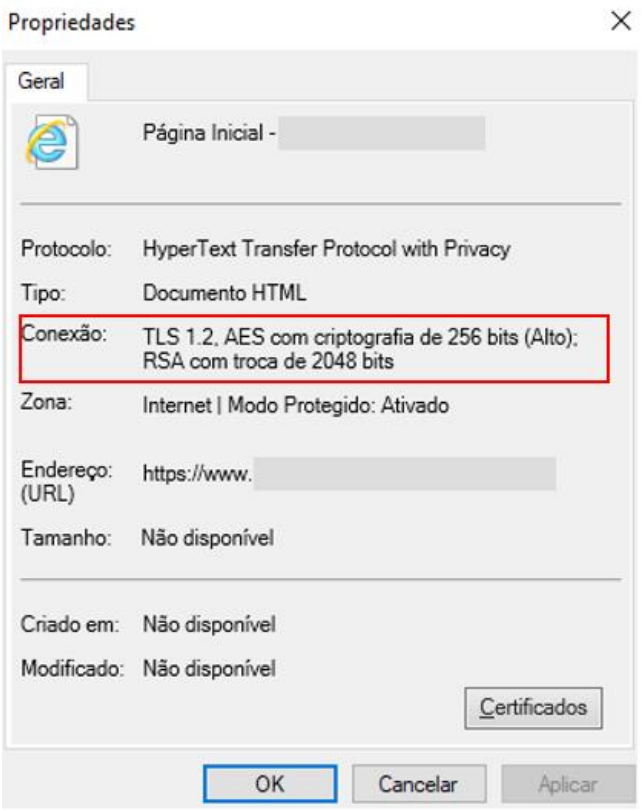
- Após clicar em “Exibir Certificados”, o browser disponibilizará as informações de validade do Certificado Digital:



- Após avaliar a validade do Certificado Digital, clicar na aba “Detalhes” e avaliar o algoritmo de criptografia, por meio do campo “Chave Pública”:



- No site do canal de relacionamento eletrônico disponibilizado pelo Participante aos seus clientes, clicar com o botão direito do mouse e em “Propriedades” avaliar se o trafego das informações é criptografado com algoritmo de criptografia, de no mínimo, 256 Bits:



- Realizar tentativa de acesso ao site do canal de relacionamento eletrônico disponibilizado pelo Participante aos seus clientes, utilizando o protocolo sem criptografia (“http”).

Nota: Em caso de fornecimento de manuais ou código fonte de sistemas para evidenciar a existência dos parâmetros de segurança de senhas, será necessário o confronto com as informações de parâmetros, coletadas diretamente nos sistemas, por meio de simulação.

3.4) Avaliação da Troca de Senha Padrão Fornecida pelos Fabricantes

A senha padrão fornecida pelo fabricante de sistemas gerenciados pelo Participante deve ser trocada.

3.4.1) Inventário e levantamento dos acessos dos bancos de dados de sistemas de escopo

Relacionar os bancos de dados que suportam sistemas dos processos de negócios do escopo de auditoria da BSM (vide etapa 8.1 deste Procedimento de Teste) e obter a relação de usuários e permissões de acesso aos bancos de dados (vide etapa 8.3 deste procedimento).

De posse da relação de usuários com acesso, identificar os usuários padrão (criados na instalação dos sistemas e dos bancos de dados) e coletar as senhas padrões de conhecimento do mercado, por meio de consulta aos fornecedores.

3.4.1) Avaliar senhas padrão de usuários

Avaliar se as senhas padrão de usuários (criados na instalação dos sistemas e dos bancos de dados) foram alteradas. São exemplos procedimentos para essa avaliação:

- Para Banco de Dados Oracle utilizar o comando "select * from dba_users_with_defpwd" indica os usuários do banco de dados que a senha padrão não foi alterada. Rodar comando "select * from select * from dba_users" e verificar quais usuários do comando anterior ainda estão ativos.

- Simular o acesso de senha padrão de usuários (criados na instalação dos sistemas e dos bancos de dados). São exemplos de usuários avaliados por meio de simulação: Usuários de Banco de Dados utilizados pelo Sinacor: "CORRWIN", "SINAWIN", "SINCORR", "DIP" e "WMSYS"; Banco de Dados SQL: usuário "sa"; e Banco de Dados Postgree: usuário "postgres".

Utilizar a relação de usuários (criados na instalação dos sistemas e dos bancos de dados), para realizar a avaliação das senhas padrão de usuários (ver pasta "Usuários – Banco de Dados" no layout de arquivos). Além desses usuários, a auditoria da BSM pode avaliar a troca de senha padrão do fabricante de outros usuários identificados durante auditoria.

3.5) Acesso Remoto aos Sistemas que Armazenam Informações de Clientes

Trabalho remoto refere-se a todas as formas de trabalho fora do escritório, incluindo ambientes de trabalho não tradicionais, como aqueles referidos como "local de trabalho flexível", "trabalho remoto" e "trabalho virtual".

Nesse modelo de trabalho, o acesso remoto à rede corporativa e aos sistemas que armazenam informações de clientes deve possuir mesmo nível de controle que o acesso realizado nas dependências do Participante (autenticação e administração dos acessos).

3.5.1) Levantamento dos controles no uso e aprovação de acesso remoto

Realizar levantamento do uso de acesso remoto à rede corporativa e aos sistemas que armazenam informações de clientes, contemplando as seguintes informações:

- Relacionar o sistema utilizado pelo Participante para acesso remoto à rede de computadores e aos sistemas dos processos de negócios do escopo de auditoria da BSM (vide etapa 8.1 deste Procedimento de Teste).

- Os procedimentos e controles existentes para administração (conceder, revogar e manter) do acesso remoto à rede de computadores e aos sistemas dos processos de negócios do escopo de auditoria da BSM, contemplando:

  a. Quem são os colaboradores, prepostos e prestadores de serviços permitidos para acesso remoto.

- Fluxo de aprovação para liberar essa forma de acesso: Como e quando o Participante concede, revoga e mantém acesso remoto aos colaboradores, prepostos e prestadores de serviços, bem como os responsáveis por essas autorizações desses acessos.

- O mecanismo de autenticação e os parâmetros de senha existentes para acesso remoto. Os requisitos de parâmetros de senha para acesso remoto devem seguir, no mínimo, segurança equivalente aos parâmetros exigidos para os sistemas internos (vide etapa 3.3 deste Procedimento de Testes).

- O controle utilizado pelo sistema de acesso remoto para tráfego de informações de forma segura. O tráfego dessas informações deve ser criptografado, como por exemplo, a utilização de VPN (*Virtual Private Network*) para acesso remoto.

3.5.2) Administração de acessos remotos

- Obter a relação de usuários e permissões de acesso remoto (vide etapa 8.3 deste Procedimento de Teste) e realizar as seguintes avaliações:

  a. Avaliar a existência de usuários com acesso remoto sem um responsável atribuído (vide etapas 8.4 e 8.5 deste Procedimento de Teste).

  b. Avaliar a existência de usuários desligados com acesso remoto ativo (vide etapa 8.6 deste Procedimento de Teste).

  c. Avaliar a existência de usuários cujo vínculo do responsável pelo usuário não foi identificado pelo Participante (vide etapa 8.7 deste Procedimento de Teste).

A avaliação sobre a segregação de funções é realizada no nível do acesso a rede de computadores e aos sistemas dos processos de negócios do escopo de auditoria da BSM, independente da forma de acesso – remoto ou interno (vide etapa 8.8 deste Procedimento de Teste).

3.5.3) Mecanismo de autenticação e os parâmetros de senha do acesso remoto

- Avaliar os requisitos de parâmetros de senha para acesso remoto e se seguem, no mínimo, segurança equivalente aos parâmetros exigidos para os sistemas internos (vide etapa 3.3 deste Procedimento de Testes).

3.5.4) Tráfego de informações seguro

- Avaliar se o trafego de informações do acesso remoto e realizada por canal seguro. Obter evidência da criptografia utilizada para o tráfego informações no sistema de acesso remoto. A comprovação do uso da criptografia para o tráfego de informações no acesso remoto permite a comunicação da informação com a rede de computadores e aos sistemas do Participante por meio seguro.

4) Processo Trilha de Auditoria nos Sistemas (Aplicativos e Negociação) e Rede de Computadores

Principais Requisitos Normativos: Itens 133 e 134 do Roteiro Básico

Documentos utilizados na Execução do Procedimento de Teste:

- Item 7: Trilhas de auditoria – dos registros de entrada/saída aos sistemas de negociação
- Item 8: Logs de ofertas (OMS x B3)
- Item 9: Logs de ofertas (Tela de negociação x OMS)
- Item 30: Trilha de auditoria da rede corporativa e dos sistemas escopo
- Item 13: Planilha de sistemas de negociação
- Item 29: Planilha de sistemas

Procedimento de Teste

4.1) Inventário dos Sistemas de Escopo

Elaborar documento relacionando (inventário) a rede de computadores e os sistemas aplicativos que suportam os processos de negócios do escopo da auditoria da BSM (Cadastro de Clientes, *Suitability*, Executar Ordens, Liquidar Negócios, Administrar Custódia de Ativos e Posições e Gerenciar Riscos. Incluir nesse inventário os sistemas de negociação e de roteamento de ordens – OMS. Esses sistemas relacionados nesse documento devem constar no Mapeamento da Infraestrutura de TI (itens 13 e 29).

4.2) Inventário das Trilhas de Auditoria dos Sistemas de Escopo

De posse desse inventário da rede de computadores e dos sistemas aplicativos que suportam os processos de negócios do escopo da auditoria da BSM (vide etapa 4.1 do Procedimento de Teste), identificar se os sistemas possuem, no mínimo, as trilhas de auditoria ativas das seguintes atividades críticas:

Processo	Atividades críticas
Cadastro de Clientes	Adesão ao Contrato de intermediação e das normas aplicáveis (em caso de adesão eletrônica) **(A)**
	Inclusão e manutenção de dados cadastrais de clientes
Custódia	Transferência de custódia de clientes

Processo	Atividades críticas
Faturamento (BM&F/Bovespa)	Alteração de corretagem
Ordens (BM&F/Bovespa)	Inclusão, alteração e cancelamento de registro de ordens de clientes
Conta Corrente e Tesouraria	Inclusão e manutenção de valores financeiros lançados manualmente na conta corrente gráfica dos clientes
Suitability	Inclusão e alteração de perfil de Investimentos de clientes
	Perguntas e respostas do questionário para composição do perfil de *suitability* (em caso de questionário eletrônico)
Risco pré-operacional	Inclusão e alteração de limites operacionais de clientes
Risco pós-operacional	Inclusão e alteração de parâmetros que compõem os limites operacionais dos clientes.
Acesso (Entrada e Saída do Sistema)	Registro dos acessos de entrada e saída (*login*/*logoff*) à rede de computadores e aos sistemas de negociação (Home Broker e DMA)
Trilha administrativa	Atividades administrativas (alteração de parâmetros, gestão de usuários, bloqueio e desbloqueio de senhas) nos sistemas de negociação.
Negociação **(B) (C)**	*Log* de envio de ofertas à B3, contendo: • Código/nome do cliente; • Sessão de negociação; • Descrição da oferta (ativo, preço, quantidade); • Tipo da oferta (compra/venda); • Status da oferta (inserida, alterada, parc. cancelada, cancelada, parc. executada, executada, rejeitada e etc.); • Data do pregão; • Data da inclusão e alteração da oferta; • Usuário (cliente, operador ou assessor) que inseriu, alterou ou cancelou a oferta; e • Endereço IP e/ou informações que permitam a identificação da localidade física do (se disponível). Nota: O log deve ser histórico, contendo todos os status das ofertas no período de auditoria solicitado."
	Log de envio de ofertas da tela de negociação ao OMS, contendo: • Código/nome do cliente; • Sessão de negociação; • Descrição da oferta (ativo, preço, quantidade); • Tipo da oferta (compra/venda); • Status da oferta (inserida, alterada, parc. cancelada, cancelada, parc. executada, executada, rejeitada e etc.); • Data do pregão; • Data da inclusão e alteração da oferta; • Usuário (cliente, operador ou assessor) que inseriu, alterou ou cancelou a oferta; e • Endereço IP e/ou informações que permitam a identificação da localidade física do (se disponível). Nota: O log deve ser histórico, contendo todos os status das ofertas no período de auditoria solicitado.

(A) Além do registro da adesão é necessário o registro do conteúdo do contrato aderido pelo cliente ou a versão do contrato aderido pelo cliente (para esse caso é necessário evidência do conteúdo da versão aderida).

(B) As trilhas referentes aos logs de ofertas (itens 8 e 9) estão dispostas separadamente. No entanto, informações requeridas em seu conteúdo em ambas podem ser representadas e apresentadas à auditoria da BSM em uma única trilha.

(C) São requeridas as trilhas de logs de ofertas (itens 8 e 9) de sistemas de negociação (OMS – Sistema de Gerenciamento de Ordens) gerenciados pelo Participante ou por terceiro por ele contratado). Não serão requeridas trilhas de sistemas de negociação

contratados pelo próprio cliente (a contratação e/ou desenvolvimento do sistema é do próprio cliente, sem gestão do Participante).

4.3) Avaliação da Suficiência das Trilhas de Auditoria

Obter as trilhas de auditoria da rede de computadores e dos sistemas (aplicativos e de negociação) (itens 7, 8, 9 e 30), das atividades listadas na etapa 4.2 do Procedimento de Teste e avaliar:

a) Se as trilhas de auditoria (E) existem e estão habilitadas e são (S) suficientes para assegurar o rastreamento do evento. Para isso devem conter no mínimo:

- Identificação do usuário
- Data e horário da ocorrência do evento
- Evento/atividades críticas
  Evento de uma trilha de auditoria é o registro de uma ação (atividade) realizada pelo usuário no sistema.

  Exemplo: Alteração do Cadastral do Cliente (alteração de estado civil)

USUARIO	DATA – HORA	OCORRENCIA	TIPO	ESTADO CIVI	NM_CONJUGE
ABC	05/02/2017 12:38	ANTERIOR	ALT	(1) SOLTEIRO	-
ABC	05/02/2017 12:38	ATUAL	ALT	(3) CASADO	MARIA JOSE SILVA

b) Para os sistemas eletrônicos de negociação (Home Broker e DMA) as trilhas devem ser (S) suficientes para assegurar o rastreamento de:

- Identificação do usuário (assessor, operador e cliente)
- Código / Nome do Cliente
- Sessão
- Descrição da ordem (ativo, preço e quantidade)
- Tipo da ordem (compra / venda)
- Todos os status da ordem
- Data Pregão
- Data inclusão, alteração e cancelamento da ordem
- Código Operador / Assessor (quando aplicável)
- Origem da Oferta (IP do usuário e/ ou forma equivalente de outros que permitam identificação da origem).

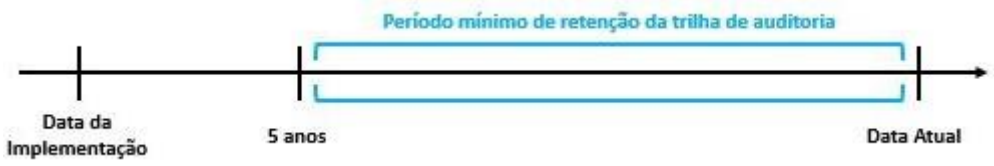
c) Para os sistemas eletrônicos de negociação (Home Broker e DMA) e rede de computadores as trilhas devem ser (S) suficientes para assegurar registro de acesso de entrada e saída (*login* / *logoff*) e conter:

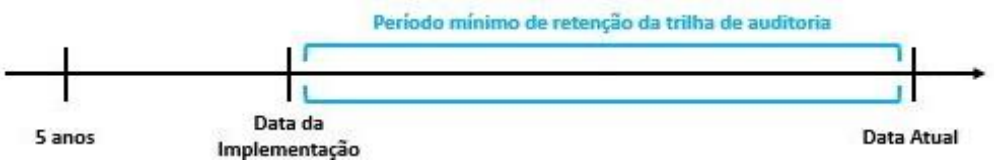
- Login do usuário (*username*);
- Data/hora do evento;
- Tipo (entrada/saída); e
- Endereço IP e/ou informações que permitam a identificação da localidade física do (se disponível).

4.4) Avaliação da Retenção das Trilhas de Auditoria

Obter as evidências do registro mais antigo (de no mínimo 5 anos ou desde a data da implantação) das trilhas de auditoria da rede de computadores e dos sistemas (aplicativos e de negociação) (itens 7, 8, 9 e 30), das atividades listadas na etapa 4.2 do Procedimento de Teste e avaliar:

Se a trilha de auditoria obtida se refere a um evento de no mínimo de 5 anos ou desde a implementação do sistema, conforme demonstrado no exemplo abaixo:





5) Processo Trilha de Auditoria nos Sistemas de Negociação (Origem da Oferta)

Principais Requisitos Normativos: Itens 54, 133 e 134 do Roteiro Básico

Documentos utilizados na Execução do Procedimento de Teste:

- Item 7: Trilhas de auditoria - dos registros de entrada/saída aos sistemas de negociação
- Item 8: Logs de ofertas (OMS x B3)
- Item 9: Logs de ofertas (Tela de negociação x OMS)
- Item 13: Mapeamento Sistemas de Negociação
- Item 14: Relação de IP (*Internet Protocol*) das estações de trabalho e servidores da matriz, filiais e AAI
- Item 15: IP do Wifi disponibilizado para clientes na matriz, filiais e AAIs

Procedimento de Teste

5.1) Inventário dos Sistemas de Negociação

Elaborar documento relacionando (inventário) os sistemas de negociação do Participante, de roteamento de ordens – OMS, bem como as sessões de negociação utilizadas por esses sistemas. Esses sistemas relacionados nesse documento devem constar no Mapeamento de Sistemas de Negociação (item 13).

5.2) Inventário dos endereços IPs pela mesa de operações e sala de clientes

Elaborar documento relacionando endereços IP (ou range de IPs utilizados) por estação de trabalho da mesa de operações (matriz e filial), bem como das salas de clientes. Utilizar como base o documento de relação de IP das estações de trabalho e servidores da matriz, filiais e AAI (item 14) e o documento de IP do Wifi disponibilizado para clientes na matriz, filiais e AAIs (item 15).

5.3) Inventário das Trilhas de Auditoria dos Sistemas de Negociação

De posse desse inventário dos sistemas de negociação do Participante (vide Etapa 5.1 do Procedimento de Teste), identificar e obter as trilhas desses sistemas de negociação do período de auditoria avaliado (ver período na planilha de *Layout* de Arquivo) desses sistemas de negociação (Itens 7, 8 e 9):

Trilha de Auditoria – Sistema de Negociação (A)
Log de envio de ofertas à B3, contendo: • Código/nome do cliente; • Sessão de negociação; • Descrição da oferta (ativo, preço, quantidade); • Tipo da oferta (compra/venda); • Status da oferta (inserida, alterada, parc. cancelada, cancelada, parc. executada, executada, rejeitada e etc.); • Data do pregão; • Data da inclusão e alteração da oferta; • Usuário (cliente, operador ou assessor) que inseriu, alterou ou cancelou a oferta; e • Endereço IP e/ou informações que permitam a identificação da localidade física do (se disponível). Nota: O log deve ser histórico, contendo todos os status das ofertas no período de auditoria solicitado."
Log de envio de ofertas da tela de negociação ao OMS, contendo: • Código/nome do cliente; • Sessão de negociação; • Descrição da oferta (ativo, preço, quantidade); • Tipo da oferta (compra/venda); • Status da oferta (inserida, alterada, parc. cancelada, cancelada, parc. executada, executada, rejeitada e etc.); • Data do pregão; • Data da inclusão e alteração da oferta; • Usuário (cliente, operador ou assessor) que inseriu, alterou ou cancelou a oferta; e • Endereço IP e/ou informações que permitam a identificação da localidade física do (se disponível). Nota: O log deve ser histórico, contendo todos os status das ofertas no período de auditoria solicitado.
Registro dos acessos de entrada e saída (*login*/*logoff*) aos sistemas de negociação (Home Broker e DMA).

(A) – As trilhas referentes aos logs de ofertas (itens 8 e 9) estão dispostas separadamente. No entanto, informações requeridas em seu conteúdo em ambas podem ser representadas e apresentadas à auditoria da BSM em uma única trilha.

– São requeridas as trilhas de logs de ofertas (itens 8 e 9) de sistemas de negociação (OMS – Sistema de Roteamento de Ordens) gerenciados pelo Participante ou por terceiro por ele contratado. Não serão requeridas trilhas de sistemas de negociação cuja a propriedade e gestão seja do cliente.

– O período requerido ao Participante das trilhas de logs de ofertas (itens 8 e 9) de sistemas de negociação (OMS – Sistema de Roteamento de Ordens) gerenciados pelo Participante ou por terceiro por ele contratado e utilizados exclusivamente pela mesa de operações e por assessores (prepostos) do Participante será de 1 dia selecionado aleatoriamente do último mês de escopo da auditoria. Para esse caso, o período das

trilhas de registros de entrada e saída de sistemas de negociação (item 7) permanece 1 mês (ver período na planilha de *Layout* de Arquivo).

5.4) Avaliação da Suficiência das Trilhas de Auditoria no Período

De posse das trilhas de auditoria no período (vide Etapa 5.3 do Procedimento de Teste) avaliar:

a) Se há registros de ofertas para todos os dias de pregão do período de auditoria do período avaliado (itens 7, 8 e 9) (ver período na planilha de *Layout* de Arquivo).

b) Destacar os campos dessas trilhas de auditoria que identificam o (i) usuário que enviou a oferta (login que acessou o sistema), (ii) o cliente (conta), (iii) a sessão de negociação utilizada e a (iv) origem da oferta (IP do usuário ou forma equivalente), e avaliar:

- A Finalidade da sessão de negociação (identificar a finalidade das sessões de negociação registradas e utilizadas na trilha de auditoria do período avaliado) e a identificação do nome do usuário que enviou a oferta (identificar na trilha de auditoria do período analisado o nome do responsável de cada usuário que enviou ofertas de clientes) devem ser realizadas nessa Etapa, conforme Procedimento de Testes da Trilha de Negociação (Uso de Sessões de Negociação).

- Se esses registros de ofertas do período de auditoria avaliados (itens 7 e 8), possuem (i) identificação da origem (IP usuário ou forma equivalente) e (ii) registros de acesso de entrada (login / logoff) correspondentes para o mesmo dia (item 9).

  Para os sistemas de negociação que possuírem origem (IP ou forma equivalente) em ambas as trilhas solicitadas (itens 7, 8 e 9), o Participante deve informar as trilhas que devem ser consideradas para avaliação da origem da oferta.

5.5) Avaliação dos Cenários Identificados nas Trilhas de Auditoria

De posse das trilhas de auditoria no período (vide Etapa 5.3 do Procedimento de Teste), da identificação da origem da oferta, da finalidade da sessão de negociação e dos nomes dos responsáveis pelos usuários que enviaram as ofertas, realizada na avaliação da

suficiência das trilhas de auditoria (vide Etapa 5.4 do Procedimento de Teste), avaliar a ocorrência dos seguintes cenários:

a) Cenário 1: Ofertas sem identificação da origem (IP do usuário ou forma equivalente)

Identificar na trilha de auditoria no período de cada sistema de negociação do Participante a existência de usuário (login que acessou o sistema) de responsabilidade de Assessor (AAI ou Assessores Bancários), Operador de Mesa, cliente final com oferta enviada à B3 sem identificação da origem (IP do usuário ou forma equivalente). Nessa situação, os campos dessas trilhas que identificam a origem estão em branco ou o sistema não possui o registro dessa informação.

b) Cenário 2: Ofertas com identificação da origem (IP do usuário ou forma equivalente) insuficientes

De posse do documento de levantamento endereços dos IP (ou range de IPs) utilizados por servidores, por estação de trabalho da mesa de operações (matriz e filial), bem como da sala de cliente (vide Etapa 5.2 do Procedimento de Teste), identificar na trilha de auditoria no período de cada sistema de negociação do Participante a existência de usuário (login que acessou o sistema) de responsabilidade de Assessor (AAI ou Assessores Bancários), Operador de Mesa, cliente final com oferta enviada à B3 com identificação da origem de servidores da rede de computadores ou que não possibilitam a identificação do equipamento utilizado pelo usuário que enviou a oferta (exemplos: roteadores / firewall).

Nessa situação, os campos dessas trilhas que identificam a origem possuem uma identificação (IP ou forma equivalente. Exemplo: IP do firewall), no entanto, essa identificação não permite determinar o equipamento utilizado pelo usuário para enviar a oferta à B3. Por tanto, o IP registrado na trilha de auditoria não diferencia se a ordem foi encaminhada de um equipamento localizado na mesa de operações do Participante ou na sala de clientes.

c) Cenário 3: Ofertas de Clientes com identificação da origem (IP do usuário ou forma equivalente) de estações de trabalho da mesa de operações e de assessores (escritório AAI e assessores bancários).

Identificar na trilha de auditoria no período de cada sistema de negociação do Participante a existência de usuário (login que acessou o sistema) de cliente final com oferta enviada à B3 com a mesma identificação da origem (IP do usuário ou forma

equivalente) da estação de trabalho utilizada por Assessor (AAI ou Assessores Bancários) e por Operador de Mesa para um mesmo dia.

Para os Participante que não possuem sala de clientes, identificar na trilha de auditoria no período de cada sistema de negociação do Participante a existência de usuário (login que acessou o sistema) de cliente final com oferta enviada à B3 com identificação da origem (IP do usuário ou forma equivalente) de estações de trabalho do Assessor (AAI ou Assessores Bancários) e Operador de Mesa. Avaliar também as situações em que se ocorra a existência usuário (login que acessou o sistema) de cliente final com oferta enviada à B3 com identificação da origem de estações de trabalho de colaboradores do Participante, que não desempenham funções de operador de mesa e assessor (para esses casos avaliar se tratam de procurador / emissor autorizado pelo cliente).

Para os Participantes que possuem sala de clientes, identificar na trilha de auditoria no período de cada sistema de negociação do Participante a existência de usuário (login que acessou o sistema) de cliente final com oferta enviada à B3 com identificação da origem (IP do usuário ou forma equivalente) de estações de trabalho localizadas na mesa de operações do Participante, utilizadas por Assessor (AAI ou Assessores Bancários) e por Operador. Utilizar como base (i). O inventário da identificação da origem das estações de trabalho de Assessor (AAI ou Assessores Bancários) e de Operador de Mesa (vide Etapa 2 do Procedimento de Teste) ou (ii). A identificação da origem das ofertas enviadas por estação de trabalho utilizada por Assessor (AAI ou Assessores Bancários) e por Operador de Mesa para um mesmo dia. Avaliar também as situações em que se ocorra a existência usuário (login que acessou o sistema) de cliente final com oferta enviada à B3 com identificação da origem de estações de trabalho de colaboradores do Participante, que não desempenham funções de operador de mesa e assessor (para esses casos avaliar se tratam de procurador / emissor autorizado pelo cliente).

6) Processo Trilha de Auditoria nos Sistemas de Negociação (Uso de Sessão)

Principais Requisitos Normativos: Itens 54, 133 e 134 do Roteiro Básico

Documentos utilizados na Execução do Procedimento de Teste:

- Item 1: Lista de Colaboradores Ativos
- Item 2: Lista de Colaboradores, Terceiros e Agentes autônomos de Investimentos desligados/distratados
- Item 3: Lista de AAIs
- Item 4: Lista de Clientes Atendidos pelos AAIs
- Item 6: Lista de usuários dos Sistemas de Negociação
- Item 7: Trilhas de auditoria - dos registros de entrada/saída aos sistemas de negociação
- Item 8: Logs de ofertas (OMS x B3)
- Item 9: Logs de ofertas (Tela de negociação x OMS)
- Item 13: Planilha de Sistemas de Negociação

Procedimento de Teste

6.1) Inventário dos Sistemas de Negociação

Elaborar documento relacionando (inventário) os sistemas de negociação do Participante, de roteamento de ordens – OMS, bem como as sessões de negociação utilizadas por esses sistemas. Esses sistemas relacionados nesse documento devem constar no Mapeamento de Sistemas de Negociação (item 13).

6.2) Inventário das Trilhas de Auditoria dos Sistemas de Negociação

De posse desse inventário dos sistemas de negociação do Participante (vide Etapa 6.1 do Procedimento de Teste), identificar e obter as trilhas desses sistemas de negociação do período de auditoria avaliado (ver período na planilha de *Layout* de Arquivo) (Itens 7, 8 e 9):

Trilha de Auditoria – Sistema de Negociação
Log de envio de ofertas à B3, contendo: • Código/nome do cliente; • Sessão de negociação; • Descrição da oferta (ativo, preço, quantidade); • Tipo da oferta (compra/venda); • Status da oferta (inserida, alterada, parc. cancelada, cancelada, parc. executada, executada, rejeitada e etc.); • Data do pregão; • Data da inclusão e alteração da oferta; • Usuário (cliente, operador ou assessor) que inseriu, alterou ou cancelou a oferta; e • Endereço IP e/ou informações que permitam a identificação da localidade física do (se disponível). Nota: O log deve ser histórico, contendo todos os status das ofertas no período de auditoria solicitado."
Log de envio de ofertas da tela de negociação ao OMS, contendo: • Código/nome do cliente; • Sessão de negociação; • Descrição da oferta (ativo, preço, quantidade); • Tipo da oferta (compra/venda); • Status da oferta (inserida, alterada, parc. cancelada, cancelada, parc. executada, executada, rejeitada e etc.); • Data do pregão; • Data da inclusão e alteração da oferta; • Usuário (cliente, operador ou assessor) que inseriu, alterou ou cancelou a oferta; e • Endereço IP e/ou informações que permitam a identificação da localidade física do (se disponível). Nota: O log deve ser histórico, contendo todos os status das ofertas no período de auditoria solicitado.
Registro dos acessos de entrada e saída (*login*/*logoff*) aos sistemas de negociação (Home Broker e DMA).

(A) – As trilhas referentes aos logs de ofertas (itens 8 e 9) estão dispostas separadamente. No entanto, informações requeridas em seu conteúdo em ambas podem ser representadas e apresentadas à auditoria da BSM em uma única trilha.

– São requeridas as trilhas de logs de ofertas (itens 8 e 9) de sistemas de negociação (OMS – Sistema de Roteamento de Ordens) gerenciados pelo Participante ou por terceiro por ele contratado. Não serão requeridas trilhas de sistemas de negociação cuja a propriedade e gestão seja do cliente.

– O período requerido ao Participante das trilhas de logs de ofertas (itens 8 e 9) de sistemas de negociação (OMS – Sistema de Roteamento de Ordens) gerenciados pelo Participante ou por terceiro por ele contratado e utilizados exclusivamente pela mesa de operações e por assessores (prepostos) do Participante será de 1 dia selecionado aleatoriamente do último mês de escopo da auditoria. Para esse caso, o período das trilhas de registros de entrada e saída de sistemas de negociação (item 7) permanece 1 mês (ver período na planilha de *Layout* de Arquivo).

6.3) Avaliação da Suficiência das Trilhas de Auditoria no Período

De posse das trilhas de auditoria no período (vide Etapa 6.2 do Procedimento de Teste) avaliar:

a) Se há registros de ofertas para todos os dias de pregão do período de auditoria do período avaliado (Itens 7, 8 e 9) (ver período na planilha de *Layout* de Arquivo).

b) Se há registros de entrada/saída aos sistemas de negociação (item 7) para todos os dias em que houveram inserção de ofertas no período avaliado (Itens 8 e 9) (ver período na planilha de *Layout* de Arquivo).

   A inserção de ofertas no período avaliado de sistemas de negociação (OMS – Sistema de Roteamento de Ordens) gerenciados pelo Participante ou por terceiro por ele contratado e utilizados exclusivamente pela mesa de operações e por assessores (prepostos) será obtida por meio de consulta às bases da B3 para posterior confronto com os registros de entrada/saída a esses sistemas (item 7).

c) Destacar os campos dessa trilha de auditoria que identificam o (i) usuário que enviou a oferta (login que acessou o sistema), (ii) o cliente (conta) e a (iii) sessão de negociação utilizada, e avaliar:

   - Finalidade da sessão de negociação: Classificar e identificar a finalidade das sessões de negociação registradas e utilizadas na trilha de auditoria do período avaliado:

     Classificação/Finalidade:

     - DMA (Cliente)
     - Mesa de Operações (Operador de Mesa)
     - Assessor (Escritório de Agente Autônomo de Investimentos, Assessor Bancário).

     A avaliação comtemplará somente registro de oferta de ativos válidos. Não avaliaremos ativos de testes nessa Etapa.

     A partir das sessões de negociação declaradas no Mapeamento de Sistemas de Negociação (item 13), confrontar com as sessões de negociação utilizadas nas trilhas de auditoria do período avaliado (Itens 8 e 9).

   - Identificar o nome do usuário que enviou a oferta: A partir da relação de usuários de sistemas de negociação disponibilizada (item 6), identificar na trilha de auditoria do período analisado o nome do responsável de cada usuário que enviou ofertas de clientes.

Após identificar o nome do responsável de cada usuário que enviou a ofertas de clientes, confrontar os nomes com o cadastro de clientes do Participante, com a lista de emissores autorizados de clientes encaminhada à B3 pelo Participante, com a Lista de Colaboradores Ativos (item 1), com Lista de Colaboradores Desligados (item 2), Lista de AAIs (item 3) e com Lista de clientes atendidos pelos AAIs (item 4) para identificar o vínculo com o cliente ou com o Participante.

Identificação do vínculo:

- Cliente (usuário do cliente)
- Emissor autorizado (usuário do emissor autorizado pelo cliente)
- Operador de Mesa (usuário do operador de mesa)
- Assessor (Usuário do Agente Autônomo de Investimentos ou assessor bancário).
- Desligado (usuário de colaborador desligado)
- Outros (usuários de colaboradores – que não se encontram nos itens acima). Destacar nessa identificação os colaboradores em férias no período avaliado.

6.4) Avaliação dos Cenários Identificados nas Trilhas de Auditoria

De posse das trilhas de auditoria no período (vide Etapa 6.2 do Procedimento de Teste) e da finalidade da sessão de negociação e dos nomes dos responsáveis pelos usuários que enviaram as ofertas, realizada na avaliação da suficiência das trilhas de auditoria (vide Etapa 6.3 do Procedimento de Teste), avaliar a ocorrência dos seguintes cenários:

a) Cenário 1: Assessores (AAI ou Assessores Bancários) e Operador de Mesa enviando ordem para cliente em sessão de Cliente Final (DMA).

Identificar na trilha de auditoria no período de cada sistema de negociação do Participante a existência de usuário (login que acessou o sistema) de responsabilidade de Assessor (AAI ou Assessores Bancários) ou Operador de Mesa enviando oferta de cliente à B3 utilizado sessão de negociação de cliente final (DMA).

Na ocorrência do cenário acima, selecionar amostra de ofertas enviadas à B3 que foram executadas desses clientes no período e solicitar ao Participante a existência da ordem do cliente.

Assessores e Operadores devem enviar ordens à B3 exclusivamente por meio de sessão de negociação Assessor e Mesa de Operações, respectivamente.

b) Cenário 2: Pessoa não autorizada enviando ordem de Cliente

Identificar na trilha de auditoria no período de cada sistema de negociação do Participante a existência de usuário (login que acessou o sistema) de responsabilidade de pessoas não autorizadas pelo cliente enviando oferta à B3.

Na ocorrência do cenário acima, selecionar amostra de ofertas enviadas à B3 que foram executadas desses clientes no período e solicitar ao Participante a existência da ordem do cliente.

O Participante deve aceitar ordens transmitidas por procurador legalmente constituído e devidamente identificado no seu cadastro de cliente.

c) Cenário 3: Clientes ou procurador autorizado pelo cliente enviando ordem em sessão de negociação Assessor ou Mesa de Operações.

Identificar na trilha de auditoria no período de cada sistema de negociação do Participante a existência de usuário (login que acessou o sistema) de responsabilidade do cliente ou procurador autorizado pelo cliente enviando oferta à B3 utilizado sessão de negociação Assessor e Mesa de Operações.

Sessão Assessor e Mesa de Operações são de uso exclusivo para envio de ordens à B3 de Assessores e Operadores, respectivamente.

d) Cenário 4: Assessores (AAI ou Assessores Bancários) e Operador de Mesa desligados (ou em férias) enviando ordens de Clientes.

Identificar na trilha de auditoria no período de cada sistema de negociação do Participante a existência de usuário (login que acessou o sistema) de responsabilidade de Assessor (AAI ou Assessores Bancários) e Operador de Mesa desligados enviando oferta de cliente à B3.

Na ocorrência do cenário acima, selecionar amostra de ofertas enviadas à B3 que foram executadas desses clientes no período e solicitar ao Participante a existência da ordem do cliente.

Colaboradores desligados do Participante que não desempenham atividades de assessor ou operador de mesa que enviaram ofertas de clientes à B3 também devem ser avaliados nessa Etapa.

Para todos os itens acima, caso a totalidade ou parte das ordens não sejam apresentadas, a amostra de ordens solicitadas poderá ser aumentada, para aprofundar análise da situação identificada.

A inserção de ofertas no período avaliado de sistemas de negociação (OMS – Sistema de Roteamento de Ordens) gerenciados pelo Participante ou por terceiro por ele contratado e utilizados exclusivamente pela mesa de operações e por assessores (prepostos) será obtida por meio de consulta às bases da B3 para posterior confronto com os registros de entrada/saída a esses sistemas (item 7) para avaliação e identificação do usuário (login que acessou o sistema) utilizados nas análises de todos os itens acima.

7) Orientação sobre Práticas de Segurança das Informações

Principal Requisito Normativo: Item 136 do Roteiro Básico

Documentos utilizados na Execução do Procedimento de Teste:

- Item 31: Evidência de divulgação das práticas de segurança das informações.

Procedimento de Teste

7.1) Aplicabilidade do Teste

O teste é aplicável para os Participantes que mantém canal de relacionamento eletrônico com os clientes utilizado para consultas (exemplo: consulta a extrato de custódia, dados cadastrais) ou transações (exemplo: alteração de dados cadastrais, preenchimento do questionário de *Suitability* e negociação).

7.2) Divulgação das práticas de segurança da informação

Avaliar se o Participante orienta os clientes sobre práticas de segurança das informações (item 31) no uso de recursos computacionais, que defina, no mínimo:

- Procedimentos de composição, guarda e troca de senha
- Riscos envolvidos no uso da Internet e métodos de prevenção
- Atualização de segurança nos computadores
- Segurança em computadores e dispositivos móveis.

8) Segurança das Informações Aplicada a Administração de Acessos

Principais Requisitos Normativos: Itens 130, 130.1.1, 130.1.4 e 137 do Roteiro Básico

Documentos utilizados na Execução do Procedimento de Teste:

- Item 1: Lista de colaboradores e terceiros ativos
- Item 2: Lista de colaboradores, AAI e terceiros desligados
- Item 3: Lista de Agentes Autônomos de Investimento
- Item 5: Lista de usuários com acesso à rede corporativa e aos sistemas aplicativos
- Item 6: Lista de usuários com acesso aos sistemas de negociação
- Item 7: Trilhas de auditoria de entrada e saída dos sistemas de negociação
- Item 8: Log de envio de ofertas à B3
- Item 10: Lista de usuários de banco de dados
- Item 12: Exceções à matriz de segregação de funções
- Item 13: Planilha de sistemas de negociação
- Item 19: Lista de responsáveis por usuários não nominais
- Item 21: Lista de usuários com acesso aos diretórios críticos
- Item 29: Planilha de Sistemas
- Item 32: Matriz de segregação de funções
- Item 33: Aprovação de acessos pelo proprietário da informação
- Item 59: Lista de usuários dos canais de recebimento de ordens
- Item 64: Lista de usuários com acesso ao diretório de áudio do sistema de gravação de voz

Procedimento de Teste

8.1) Inventário dos Sistemas de Escopo

Relacionar a rede de computadores e os sistemas aplicativos e banco de dados que suportam os processos de negócios do escopo da auditoria da BSM (Cadastro de Clientes, *Suitability*, Executar Ordens, Liquidar Negócios, Administrar Custódia de Ativos e Posições, Gerenciar Riscos, Conta Margem e Supervisão de Operações e Ofertas e Prevenção à Lavagem de Dinheiro), sistemas de roteamento de ordens e sistemas de mensageria e de gravação de voz utilizados para receber ordens de clientes. Esses sistemas relacionados devem constar na planilha de sistemas (item 29) e planilha de sistemas de negociação (item 13).

8.2) Inventário de Diretórios Escopo

Relacionar os diretórios que possuem informações sensíveis (dados de custódia de clientes, informações cadastrais e gravações de ordens) e que devem ter acesso controlado. Esses diretórios relacionados devem ser listados nos itens 21 e 64.

8.3) Levantamento dos acessos aos sistemas escopo

Para o escopo identificado (vide etapas 8.1 e 8.2 deste Procedimento de Teste), obter a relação de usuários e permissões de acesso aos sistemas aplicativos, incluindo os sistemas para acesso remoto (item 5), sistemas de negociação (item 6), bancos de dados (item 10), canais de recebimento de ordens (item 59) e diretórios críticos utilizados para armazenar informações sensíveis (itens 21 e 64).

8.4) Identificação dos responsáveis pelos usuários não nominais (genéricos) e da ciência dessa atribuição pelo responsável pelo usuário não nominal (genérico)

Avaliar o processo de atribuição de responsabilidade pelos usuários não nominais (item 19), se definido pelo Participante, com acesso aos sistemas aplicativos, incluindo os sistemas para acesso remoto, sistemas de negociação, bancos de dados, canais de recebimento de ordens, redes corporativas e diretórios que suportam os processos de negócio relacionados ao escopo da auditoria da BSM. Verificar se o processo registra e identifica o usuário (*login*), o sistema, o responsável pelo usuário e, no mínimo, a aprovação do proprietário da informação e a ciência do usuário responsável.

8.5) Verificação da existência de usuários genéricos sem um responsável atribuído

De posse relação de usuários e permissões de acesso (vide etapa 8.3 deste Procedimento de Teste), consultar a lista de colaboradores e terceiros ativos (item 1), lista de

colaboradores e terceiros desligados (item 2) e lista de agentes autônomos de investimento (item 3). Caso existam usuários de sistemas não identificados na consulta e que não estejam relacionados na identificação de responsáveis por usuários genéricos (vide etapa 8.4 deste Procedimento de Teste), esses usuários são classificados como usuários genéricos sem responsável atribuído.

8.6) Verificação da existência de usuários desligados

De posse relação de usuários e permissões de acesso (vide etapa 8.3 deste Procedimento de Teste), consultar a lista de colaboradores e terceiros desligados (item 2). Caso existam usuários de sistemas identificados na lista de colaboradores e terceiros desligados, esses usuários são classificados como colaboradores desligados com acesso ativo a sistemas.

8.7) Verificação da existência de usuários sem vínculo com o Participante

De posse relação de usuários e permissões de acesso (vide etapa 8.3 deste Procedimento de Teste), consultar a lista de colaboradores e terceiros ativos (item 1), lista de colaboradores e terceiros desligados (item 2) e lista de agentes autônomos de investimento (item 3). Caso existam usuários de sistemas que por meio da lista de acessos é possível identificar o nome do colaborador, mas não constam nas listas (itens 1, 2 e 3) e o Participante não demonstra qual o vínculo do responsável pelo usuário, esses usuários são classificados como usuários cujo vínculo do responsável não foi demonstrado pelo Participante.

8.8) Segregação de Funções: Exemplos de Matrizes de Segregação de Funções (item 32)

Não existe fórmula única para definição e documentação das atividades que acumuladas e executadas pela mesma pessoa no sistema que possam gerar conflitos de interesses e acessos em desacordo com a função desempenhada – matriz de segregação de funções.

As informações sobre segregação de funções (Matriz e outras) devem possibilitar a avaliação precisa da compatibilidade dos acessos solicitados, previamente à concessão de acesso, em relação às regras de segregação de funções definidas pelo Participante.

Seguem exemplos de formatos de Matrizes de Segregação de Funções:

I - Áreas / Função x Atividades Permitidas

Nesse modelo são elencadas todas as atividades consideradas críticas e todas as áreas/funções dos colaboradores que executam ou visualizam dados relacionados a essas atividades.

Áreas / Atividades	BACKOFFICE	CADASTRO	MESA DE OPERAÇÕES	RISCO	TECNOLOGIA DA INFORMAÇÃO
ADMINISTRAÇÃO	-	-	-	-	EDIÇÃO
ALTERAÇÃO DE CORRETAGEM	EDIÇÃO	EDIÇÃO	CONSULTA	-	-
CADASTRO DE CLIENTE	EDIÇÃO	EDIÇÃO	CONSULTA	CONSULTA	-
CADASTRO LIMITE PRÉ	-	-	-	EDIÇÃO	-
GERENCIAMENTO DE USUÁRIOS	-	-	-	-	EDIÇÃO
OPERAÇÃO	-	-	EDIÇÃO	-	-
TRANSFERÊNCIA DE CUSTÓDIA	EDIÇÃO	-	-	-	-

Observações:

a) Nesse modelo é necessário documento complementar com a indicação dos perfis utilizados para execução de cada atividade crítica em cada sistema. Segue exemplo de documento complementar:

Sistema de negociação		
Perfil	**Área**	**Transações críticas (atividades)**
Operação	Mesa de operações	Inclusão, alteração e cancelamento de ofertas e ordens de clientes;
Administrador	TI	Atividades administrativas de sistemas (alteração de parâmetros, gestão de usuários, bloqueio e desbloqueio de senhas)
Limites e Cancelamento de ofertas	Risco	Inclusão e alteração de parâmetros que compõem os limites operacionais dos clientes / Inclusão e alteração de limites operacionais de clientes / cancelamento de ofertas e ordens de clientes
Sistema de Cadastro		
Perfil	**Área**	**Transações críticas (atividades)**
Alterações cadastrais	Cadastro / *Back Office*	Inclusão e manutenção de dados cadastrais de clientes
Administrador	TI	Atividades administrativas de sistemas (alteração de parâmetros, gestão de usuários, bloqueio e desbloqueio de senhas)
Consulta	Risco / Mesa de operações / *Compliance*	Consulta de dados cadastrais

b) No mínimo, todas as atividades críticas, conflitos mínimos e áreas devem estar mapeadas na matriz e de acordo com as áreas definidas na área de Recursos Humanos.

II - Áreas / Função x Sistemas / Perfis Permitidos

Sistemas / Áreas	CADASTRO	BACKOFFICE	MESA DE OPERAÇÕES	RISCO	TECNOLOGIA DA INFORMAÇÃO
Sistema de Backoffice	Perfil: CADASTRO	Perfil: BACKOFFICE	Perfil: CONSULTA	Perfil: CONSULTA	Perfil: ADMINISTRADOR
Sistema de Cadastro de Cliente	Perfil: CADASTRO	-	Perfil: CONSULTA	Perfil: CONSULTA	Perfil: ADMINISTRADOR
Sistema de Custódia	-	Perfil: BACKOFFICE	-	-	Perfil: ADMINISTRADOR
Sistema de Negociação	-	-	Perfil: OPERAÇÃO	Perfil: RISCOS	Perfil: ADMINISTRADOR
Sistema de Risco Pré	-	-	-	Perfil: RISCOS	Perfil: ADMINISTRADOR

Observações:

a) Importante avaliar se as áreas/funções mapeadas na matriz estão de acordo com as áreas definidas no RH e se todas as áreas aplicáveis estão mapeadas na matriz.

b) Todos os sistemas e perfis utilizados pelos colaboradores do Participante devem constar na matriz.

III - Atividades que acumuladas podem gerar conflitos de interesse

Funções	Cadastro de Cliente	Inclusão, alteração e cancelamento de ofertas e ordens de clientes	Inclusão e alteração de Perfil de Investimentos de clientes	Transferência de custódia de clientes	Atividades administrativas de sistemas
Inclusão e manutenção de dados cadastrais de clientes	-	Consulta	Consulta	Conflito	Conflito
Inclusão, alteração e cancelamento de ofertas e ordens de clientes	Consulta	-	Conflito	Conflito	Conflito
Inclusão e alteração de Perfil de Investimentos de clientes	Consulta	Conflito	-	Consulta	Conflito
Transferência de custódia de clientes	Conflito	Conflito	Consulta	-	Conflito
Atividades administrativas de sistemas	Conflito	Conflito	Conflito	Conflito	-

Observação:

a) Todas as atividades críticas e conflitos mínimos devem estar mapeados na matriz.

b) O propósito desse modelo de matriz é evitar o Conflito de Interesses. Para concessão de acesso de acordo com a função desempenhada, conforme requerido também pelo Roteiro Básico, as matrizes a) e b) acima, são exemplos que atendem à essa questão.

Obs: Matrizes de segregação de funções que definem os acessos pertinentes por colaborador (nominal) não são recomendadas pois exigem alto grau de manutenção em virtude da movimentação de colaboradores e requerem atenção em casos de diferenças de acessos concedidos para colaboradores de uma mesma área com mesma função.

Além disso, casos de novos acessos (ou admissão de novo colaborador) devem estar previstos na matriz antes da concessão do acesso e não ser concedido de forma julgamental, sem consultada prévia da matriz.

8.8.1) Segregação de Funções: Avaliação da suficiência da Matriz de Segregação de Funções (item 32).

A matriz de segregação de funções deve ter informação suficiente para que as solicitações de acessos sejam confrontadas com a matriz e não haja dúvidas nessa análise ou qualquer julgamento, ou seja, a matriz de segregação deve ser suficiente para que qualquer pessoa que realize o confronto entre o acesso solicitado e o acesso permitido na matriz, chegue no mesmo resultado.

Na definição da matriz de segregação de funções e dos acessos pertinentes por função/área, é importante avaliar se os colaboradores com acessos a atividades sujeitas a certificação estão/serão certificados para tal.

Seguem aspectos que devem ser considerados na elaboração da matriz de segregação de funções em relação à suficiência:

a) Abrangência de, no mínimo, todos os sistemas escopo da auditoria da BSM (sistemas aplicativos, sistemas de negociação, bancos de dados, canais de recebimento de ordens e diretórios).

b) As áreas e/ou funções da matriz devem possuir relação direta ou ser informado uma equivalência com as áreas estabelecidas pela área de Recursos Humanos do Participante.

c) No mínimo, as seguintes atividades críticas devem estar relacionadas na matriz:

- Inclusão, alteração e cancelamento de ofertas e ordens de clientes;
- Alteração de corretagem;

- Inclusão e manutenção de valores financeiros lançados manualmente na conta corrente gráfica dos clientes;
- Transferência de custódia de clientes;
- Inclusão e manutenção de dados cadastrais de clientes;
- Inclusão e alteração de Perfil de Investimentos de clientes/questionário;
- Inclusão e alteração de parâmetros que compõem os limites operacionais dos clientes;
- Inclusão e alteração de limites operacionais de clientes;
- Atividades administrativas de sistemas (alteração de parâmetros, gestão de usuários, bloqueio e desbloqueio de senhas e download de gravação / mensageria – sistema de gravação de voz / mensageria);

d) No mínimo, os seguintes conflitos, devem estar relacionados na matriz:

- Transferência de custódia de clientes por profissional que desempenhe atividades de Operador (inserção, alteração e cancelamento de ofertas de clientes).
- Atualização de dados bancários de clientes por profissional responsável pela liquidação (pagamento e recebimento de valores de clientes).
- Inclusão e alteração de limites pré-operacionais de clientes por profissionais que desempenhe atividades de Operador (inserção, alteração e cancelamento de ofertas de clientes).

8.8.2) Segregação de Funções: Levantamento dos acessos compatíveis em caso de insuficiência da matriz de segregação de funções (item 32)

Para as insuficiências identificadas na matriz de segregação de funções e para validação dos acessos pertinentes aos bancos de dados e diretórios de rede com dados críticos, a BSM realiza um levantamento dos acessos previstos com os responsáveis indicados e validados pelo Participante.

8.8.3) Segregação de Funções: Inventário dos acessos concedidos em caráter de exceção à matriz de segregação de funções

Relacionar os acessos a sistemas concedidos em caráter de exceção à matriz de segregação de funções. Esses acessos devem constar em Exceções à matriz de segregação de funções (item 12).

Caso a matriz possua acessos em exceção / acessos conflitantes, os seguintes aspectos são considerados:

- Os acessos concedidos devem estar de acordo com o modelo de negócios e desempenho das atividades críticas realizadas pelos colaboradores;
- Monitoração da utilização dos acessos concedidos em caráter de exceção, como por exemplo, estabelecer periodicidade para avaliar as trilhas de auditoria e transações realizadas utilizando os acessos que são conflitantes/incompatíveis;
- O fluxo de aprovação de um acesso em exceção deve ser diferente, superior, do fluxo de aprovação de um acesso compatível com a matriz de segregação de funções.

8.8.4) Segregação de Funções: Confronto entre a matriz de segregação de funções/levantamento x acessos concedidos

a) Identificação do vínculo dos responsáveis pelos acessos aos sistemas concedidos

De posse relação de usuários e permissões de acesso (vide etapa 8.3 deste Procedimento de Teste), consultar a lista de colaboradores e terceiros ativos (item 1), lista de colaboradores e terceiros desligados (item 2) e lista de agentes autônomos de investimento (item 3), afim de identificar, para cada acesso ao sistema ou diretório, o vínculo do responsável.

b) Mapeamento dos acessos aos sistemas permitidos para os colaboradores e terceiros ativos

De posse do vínculo dos responsáveis pelos acessos aos sistemas (vide etapa 8.8.4.a deste Procedimento de Teste), da matriz de segregação de funções (item 32) e, em caso de insuficiência, do levantamento dos acessos compatíveis (vide etapa 8.8.2 deste Procedimento de Teste) e do inventário dos acessos concedidos em caráter de exceção à matriz de segregação de funções (vide etapa 8.8.3 deste Procedimento de Teste), mapear os acessos a sistemas permitidos para os colaboradores e terceiros ativos (item 1).

c) Identificação de acesso concedidos em desacordo com a matriz de segregação de funções ou com o levantamento dos acessos compatíveis

Confrontar a relação de usuários e permissões de acesso (vide etapa 8.3 deste Procedimento de Teste) com o mapeamento dos acessos aos sistemas permitidos para os colaboradores e terceiros ativos (vide etapa 8.8.4.b deste Procedimento de Teste). Caso existam divergência nesse confronto, esses acessos são classificados

como acessos concedidos em desacordo com a matriz de segregação de funções ou com o levantamento dos acessos compatíveis.

Fórmula do Teste de acesso incompatível:

Acessos em desacordo com a matriz de segregação de funções ou levantamento* =
Matriz de segregação de funções + Levantamento (vs) Acessos concedidos – Exceções

(*) Mapeamento dos colaboradores responsáveis pela realização de atividades críticas

8.8.5) Segregação de Funções: Materialização dos acessos incompatíveis

Com o resultado dos acessos concedidos em desacordo com a matriz de segregação de funções ou com o levantamento dos acessos compatíveis (vide etapa 8.8.4.b deste Procedimento de Teste) consultar as trilhas de auditoria (item 7) e *logs* de envio de ofertas à B3 (item 8), afim de identificar a materialização por meio da utilização desses acessos.

8.8.6) Avaliação da suficiência do processo de concessão de acessos

Avaliar se o processo de concessão de acessos acesso a sistemas, bancos de dados e redes definido pelo Participante, contempla as etapas de aprovação do acesso, no mínimo, pelo proprietário da informação (item 33) e se os acessos são concedidos somente a profissionais que possuam vínculo com o Participante (vide etapa 8.8.4.a deste Procedimento de Teste).

8.8.7) Avaliação do processo de concessão de acessos

De posse da relação de usuários e permissões de acesso (vide etapa 8.3 deste Procedimento de Teste), selecionar amostra de colaboradores e solicitar evidências do fluxo de concessão de acessos (mínimo aprovação dos acessos concedidos pelo proprietário da informação (item 33), conforme processo de concessão de acessos definido pelo Participante.

8.9) Descarte e Manutenção Segura de Dados e Equipamentos

O Participante deve possuir procedimento em que dados de clientes em documentos impressos, em mídias ou em equipamentos, sejam descartados de forma segura, quando não forem mais necessários.

Realizar levantamento do procedimento do Participante para descarte seguro de documentos impressos contendo dados de clientes, por exemplo: fragmentadoras. O procedimento adotado pelo Participante, deve inibir a reconstrução do material.

Realizar levantamento do procedimento do Participante para descarte seguro de mídias e equipamentos (cartão SD, HD, DVD, CD, *pendrive*, computadores e celulares corporativos) contendo dados de clientes. A expectativa é a realização da limpeza permanente dos dados (exemplo: "WIPE") de forma a impedir a recuperação da informação.

Para os procedimentos acima realizar *walkthrough* junto ao Participante para garantir o descarte seguro. Caso o descarte seja realizado por fornecedor, solicitar o contrato firmado para a execução da atividade e avaliar se atende e se está conforme Item 19 do Procedimento de Testes (avaliação de contratos).

9) Segurança da Rede

Principal Requisito Normativo: Itens 138, 130.1, 130.2.1, 130.2.2 e 130.3 do Roteiro Básico

Documentos utilizados na Execução do Procedimento de Teste:

- Item 71: Topologia de rede
- Item 34: Ferramenta de firewall
- Item 77: Documentação das análises e ações tomadas
- Item 78: Avaliação das vulnerabilidades e ameaças da rede de computadores

Procedimento de Teste

9.1) Análise da Topologia de Rede

Tendo como base a topologia de rede (item 71) do Participante, identificar a disposição dos firewalls para garantir que os fluxos de dados com meios externos (redes de terceiros e Internet) sejam controlados.

9.2) Registro dos Parâmetros de Alertas das Regras de *Firewall*

Analisar as configurações dos firewalls (item 34) utilizados pelo Participante, afim de identificar as regras aplicadas, interfaces monitoradas, logs e alertas.

9.3) Monitoramento da Segurança da Rede

Identificar se o Participante possui monitoramento contínuo (a) dos alertas gerados pelos dispositivos de segurança de rede (no mínimo, *firewall*); e (b) da situação (instalação e atualização das vacinas) dos softwares antivírus nas estações de trabalho e nos servidores da rede de computadores.

A frequência mínima desse monitoramento acima é semanal.

9.3.1) Escopo do Monitoramento

a. Para os Dispositivos de Rede: Identificar e obter do Participante que as seguintes monitorações são realizadas em frequência semanal (no mínimo):

- Tráfego em Portas “incomuns” (portas não conhecidas pelo mercado).
- Acesso a sites da *web* sem classificação ou de segurança duvidosa.
- Tentativas de acessos indevidos aos dispositivos de rede (no mínimo, *firewall*).

b. Para os softwares antivírus: Identificar e obter do Participante que as seguintes monitorações são realizadas em frequência semanal (no mínimo):

- Estações de trabalho e servidores da rede de computadores com software antivírus desatualizado (vacina disponibilizada pelo fornecedor).
- Remoção de softwares antivírus (ou tentativas) em estações de trabalho e servidores da rede de computadores.
- Estações de trabalho e servidores contaminados (suspeitos).

A identificação se há antivírus instalado e atualizado por meio de amostra é realizado pela auditoria da BSM na Etapa 21 deste Procedimento de Teste.

O Participante deve possuir procedimento para tratamento das situações encontradas no monitoramento da segurança da rede. A avaliação desse tratamento é realizada na Etapa 9.4 deste Procedimento de Teste.

9.4) Tratamento das Situações Encontradas no Monitoramento da Segurança da Rede

O Participante deve possuir procedimento para tratamento das situações encontradas no monitoramento da segurança da rede, que contemple o registro da (a) análise e da (b) ação tomada para resolução do incidente.

9.5) Identificação e Análise

Identificar o procedimento para identificação e análise das situações encontradas no monitoramento da segurança. Esse procedimento para análise deve contemplar, no mínimo, o registro e a análise da causa e do impacto para os processos do Participante.

9.5.1) Ação Tomada

Identificar o procedimento para resolução do incidente para as situações encontradas no monitoramento da segurança. Esse procedimento para resolução do incidente deve contemplar, no mínimo, o registro da solução do incidente (contenção, erradicação e recuperação).

9.5.2) Amostra

Obter do Participante os registros das análises (últimas 3 monitorações - controle mínimo, semanal) e das ações tomadas das situações encontradas no monitoramento da segurança (item 77).

9.6) Avaliação Periódica de Ameaças e Vulnerabilidades

Identificar se o Participante realizou a avaliação, das ameaças e vulnerabilidades da rede de computadores (item 78), no mínimo anual, e avaliar se contemplar: (a) Infraestrutura avaliada (rede de computadores e sistemas escopo da auditoria da BSM); (b) Identificação e análise dos riscos (ameaças e vulnerabilidades); e (c) Ações para o tratamento dos riscos.

Como a frequência mínima do programa esperada é anual, e a vigência do requisito é a partir de janeiro de 2019, a Avaliação Periódica poderá ser avaliada pela suficiência do desenho do programa (ainda não aplicado).

9.7) Controles para Cópia (transferência) de Informações de Clientes em Dispositivos

Identificar o procedimento do Participante para cópia (transferência) de informações de clientes oriunda de seus sistemas em dispositivos não controlados pela empresa, como por exemplo: *pendrive,* CD, DVD, smartphones e notebooks.

O Participante deve garantir o sigilo das informações de clientes mantidas sob sua guarda, desta forma, a cópia para dispositivos deve ser controlada pelo Participante.

Além do compromisso dos colaboradores, prepostos e prestadores de serviços de não realizarem cópias (transferência) para esses dispositivos (por exemplo: termos ou contratos assinados), o Participante deve possuir controles preventivos ou detectivos para essas cópias, que são exemplos:

- Bloqueio para cópia de informações em dispositivos não controlados pelo Participante.
- Permissão (temporário ou não) para cópia de informações em dispositivos não controlados pelo Participante com controle detectivo (trilha de auditoria) para o rastreamento das responsabilidades. Para esses casos a permissão é concedida para um número restrito de profissionais.

O teste sobre o controle para cópia (transferência) de informações de clientes será avaliado pela auditoria da BSM, conforme procedimento definido pelo Participante.

10) Centro de Processamento de Dados (CPD)

Principal Requisito Normativo: Item 139 do Roteiro Básico

Documentos utilizados na Execução do Procedimento de Teste:

- Item 1: Lista de colaboradores ativos
- Item 2: Lista de colaboradores desligados
- Item 3: Lista de AAIs
- Item 35: Relação de usuários ao(s) CPD(s)
- Item 36: Visita ao CPD de produção e de contingência

Procedimento de Teste

10.1) Escopo de análise

Identificar o(s) CPD(s) utilizado(s) pelo Participante como ambiente de produção e contingência localizado(s) na matriz, filial(ais) ou fornecedor(es) terceiro(s), dos sistemas e banco de dados escopo da auditoria da BSM e que possuam links de comunicação com a B3.

10.2) Avaliação dos controles de cada ambiente

Em visita realizada(s) no CPD(s) do Participante (item 36), quando aplicável(eis), avaliar a presença de material de fácil combustão, assim como os controles ambientais e de acesso (item 35) de cada ambiente, conforme abaixo:

Controle	Exemplos
Detecção e combate a incêndio	Extintor CO2 na validade, GAS FM200, alarme de incêndio, detector de fumaça e porta corta-fogo
Controle de monitoramento de temperatura e umidade	Monitoramento do medidor de temperatura e medidor de umidade
Fonte de energia alternativa	*Nobreak*, geradores, dentre outros que permitam a conclusão das atividades operacionais em curso, incluindo a realização das rotinas de *backup*.
Controle de Acesso (acesso restrito e controlado)	Dispositivo de reconhecimento biométrico, leitor de cartão magnético (crachás), dispositivo de abertura por senhas, câmeras de monitoramento, chave convencional e controle de registro dos acessos ao ambiente, identificando: data, horário e profissional

10.3) Permissões de acesso ao ambiente do CPD

Tendo como base mapeamento realizado dos colaboradores que possuem autorização de acesso ao(s) CPD(s), identificar os colaboradores com acesso (itens 1, 2 e 3) e avaliar se os acessos concedidos ao(s) CPD(s) estão de acordo (item 35).

B. CONTINUIDADE DE NEGÓCIOS

11) Pronto Atendimento aos Clientes nos Casos de Suspensões no Atendimento pela *Internet*

Principal Requisito Normativo: Item 140 do Roteiro Básico.

Documentos utilizados na Execução do Procedimento de Teste:

- Item 37: Plano de Continuidade dos Negócios; e
- Item 38: Divulgação para os clientes dos procedimentos adotados no caso de suspensão no atendimento pela Internet.

Procedimento de Teste

11.1) Avaliação da estratégia de pronto atendimento

Avaliar a existência, a divulgação e a suficiência do procedimento adotado pelo Participante (item 38) para preservar o pronto atendimento dos clientes para recebimento de ordens em caso de suspensões no atendimento pela Internet.

12) Plano de Continuidade dos Negócios (PCN)

Principal Requisito Normativo: Item 141 do Roteiro Básico.

Documentos utilizados na Execução do Procedimento de Teste:

- Item 36: Visita ao CPD e ambiente de contingência;
- Item 37: Plano de Continuidade dos Negócios;
- Item 39: Sincronização dos bancos de dados (produção x contingência); e
- Item 41: Teste do PCN.

Procedimento de Teste

12.1) Suficiência da estratégia de continuidade dos negócios

Tendo como base o Plano de Continuidade dos Negócios (PCN) definido pelo Participante (item 37) e o entendimento do processo validado pelo Participante, avaliar se a estratégia definida atende aos seguintes objetivos mínimos de recuperação:

(i). Liquidação com a B3, mecanismos que garantam:

- Recebimento e pagamento dos valores de liquidação;
- Entrega e recebimento de ativos;
- Autorização de movimentação de ativos; e
- Atendimento de chamada de margem.

(ii). Liquidação com os clientes, mecanismos que garantam:

- Comunicação com os clientes, com a B3, com o Participante de Negociação, com o Participante de Negociação Pleno, com o Participante de Liquidação, com o Agente de Custódia, com o Membro de Compensação e liquidante; e
- Monitoramento de entrada e saída de recursos.

(iii). Atualização de posições, mecanismos que garantam:

- Capacidade de encerrar posições na B3; e
- Operações realizadas em D+0 (confirmação de ordens, alocação de operação e repasse da operação).

Adicionalmente, avaliar se o PCN possui definição das seguintes informações:

- Estratégia de contingência (liquidar e/ou continuar a operação);
- Informações dos principais contatos no caso de incidentes;
- Endereços dos locais utilizados na contingência;
- Processos, infraestrutura e sistemas contingenciados; e
- Definição do plano de teste, tempos de recuperação e principais cenários de indisponibilidade, incluindo o cenário de indisponibilidade total da infraestrutura principal (instalações, sistemas e conexões).

12.2) Suficiência da infraestrutura de continuidade dos negócios

Tendo como base os sistemas aplicativos, infraestrutura e sistemas de negociação definidos pelo Participante como infraestrutura necessária para atendimento da estratégia de continuidade dos negócios, avaliar se os procedimentos de atualização dos sistemas (item 39), entre os ambientes de produção e contingência, se aplicável, estão implantados de acordo com a estratégia definida, de forma a garantir que as operações possam ser continuadas em ambiente de contingência.

Avaliar a infraestrutura de TI implementada no ambiente de contingência (item 36), afim de assegurar que o ambiente suporte a estratégia do Participante:

- Sistemas contingenciados para liquidação e atualização de posições (replicação, sincronização, conectividade);
- Infraestrutura de centro de processamento de dados (CPD) de contingência;
- Local de trabalho de contingência (quantidade de posições, *softwares* instalados); e
- Links de comunicação de contingência (comunicação com a B3 e com a produção).

12.3) Testes do PCN

Avaliar se o Participante realizou testes do PCN (item 41), no mínimo anualmente, e verificar o escopo dos testes (liquidação e atualização de posições), as pessoas envolvidas, se todos os sistemas previstos para serem utilizados em contingência foram testados, ambientes utilizados e os resultados. Assegurar que os testes realizados têm como base o cenário de indisponibilidade total da infraestrutura de TI de produção, e que as atividades (liquidação e atualização) foram realizadas a partir da infraestrutura de TI de contingência.

Tipos de evidências apresentadas:

- Prints de tela que demonstrem a infraestrutura de contingência.

(Exemplos: Print evidenciando a utilização do ambiente – aplicações e banco de dados – de contingência; e Print evidenciando a restauração da cópia de segurança em ambiente de contingência).

- Trilhas de auditoria das ações efetuadas na infraestrutura de contingência.

(Exemplo: Log evidenciando a utilização do banco de dados de contingência nos testes).

- Evidência de toda a infraestrutura avaliada em ambiente de contingência.

(Exemplo: Print da solução de replicação demonstrando a troca de infraestrutura: desativação do ambiente de produção e habilitação do ambiente de contingência).

As evidências de testes de continuidade dos negócios devem comprovar o acesso aos sistemas críticos e a realização das principais transações previstas no PCN nesses sistemas, após a subida do banco de dados de contingência.

C. MONITORAMENTO E OPERAÇÃO DA INFRAESTRUTURA DE TI

13) Monitoramento da infraestrutura de TI

Principais Requisitos Normativos: Itens 142 e 146 do Roteiro Básico.

Documentos utilizados na Execução do Procedimento de Teste:

- Item 29: Planilha de sistemas;
- Item 42: Planilha de mapeamento infraestrutura;
- Item 43: Relatório de latência e disponibilidade dos sistemas de negociação;
- Item 44: Monitoramento da disponibilidade, da capacidade e do desempenho;
- Item 66: Planilha de serviços de TI; e
- Item 71: Topologia de rede.

Procedimento de Teste

13.1) Avaliação dos procedimentos de monitoramento da disponibilidade e latência dos sistemas de negociação

Tendo como base o mapeamento dos sistemas de negociação disponibilizados pelo Participante a seus clientes (exemplo: *Home Broker*, DMA I e DMA II) (itens 29 e 42), avaliar o monitoramento para todos esses sistemas, dos indicadores de disponibilidade e latência para período de 3 meses (item 43).

13.2) Análise do monitoramento da disponibilidade, da capacidade e do desempenho da infraestrutura de TI

Tendo como base o mapeamento de sistemas e servidores (itens 29 e 42) realizado durante a auditoria, avaliar o monitoramento preventivo (item 44) realizado da disponibilidade, da capacidade e do desempenho (processador, disco rígido e memória RAM) de todos os servidores de produção que suportam os sistemas aplicativos, inclusive sistemas de negociação e respectivos bancos de dados.

13.3) Análise do monitoramento da disponibilidade dos canais de comunicação

Tendo como base a topologia de rede do Participante (item 71) e o mapeamento dos canais de comunicação - *links* (item 66) realizado durante a auditoria, avaliar se os procedimentos de monitoramento preventivo (item 44) de disponibilidade abrangem todos os canais de comunicação utilizados pelo Participante, como: *links* de comunicação com a B3 (RCB/RCCF) e links de comunicação entre localidades do Participante (*lan-to-lan*).

14) Execução, monitoramento e armazenamento externo de cópias de segurança (*backups*)

Principais Requisitos Normativos: Itens 143, 144 e 145 do Roteiro Básico

Documentos utilizados na Execução do Procedimento de Teste:

- Item 7: Trilhas de auditoria dos registros de entrada/saída aos sistemas de negociação;
- Item 30: Trilha de auditoria da rede corporativa e dos sistemas escopo);
- Item 45: Política, normas e procedimentos de *backup;*
- Item 46: Evidência das rotinas de *backup* agendadas;
- Item 47: Log de execução dos *backups;*
- Item 48: Procedimento de registro e de solução das falhas na execução dos *backups;*
- Item 49: Teste de restauração de mídias de *backup;*
- Item 50: Armazenamento externo das mídias de *backup;*
- Item 51: Inventário das mídias de *backup;*
- Item 61: Evidência de retenção de todo(s) o(s) canal(ais) de recebimento de ordens de clientes (exemplo: gravação de voz e mensageria); e
- Item 67: Cópia dos contratos estabelecidos com os fornecedores de TI.

Procedimento de Teste

14.1) Análise da documentação dos procedimentos e rotinas de *backup*

Avaliar se o Participante possui procedimentos documentados das rotinas de *backup* de dados e de ordens de clientes (item 45), que sejam acessíveis e de pleno conhecimento dos responsáveis pelo processo, e se definem, no mínimo, as seguintes diretrizes:

- Responsáveis;
- Escopo;
- Frequência;
- Método (ferramenta);
- Monitoração;
- Testes (periodicidade, escopo e resultado);
- Local de armazenagem (acessos e controles ambientais);
- Controles no transporte das mídias;
- Período de retenção das mídias; e
- Inventário das mídias.

14.2) Análise do escopo e da frequência da configuração das rotinas de *backup*

Tendo como base mapeamento realizado junto ao Participante da ferramenta utilizada no *backup*, avaliar se a execução da(s) rotina(s) de *backup*(s) (item 46) ocorre diariamente, na matriz, filial(ais), preposto(s) e se contemplam todo o escopo de sistemas/dados/voz avaliados:

- Bancos de dados dos sistemas aplicativos e de negociação (DMA I) que suportam os seguintes processos:
  - Ordens;
  - Cadastro;
  - Risco (registro das extrapolações dos limites de risco, inclusão e alteração de limites operacionais);
  - Custódia;
  - Liquidação (movimentações em conta-corrente);
  - Conta margem (movimentações em conta margem, registro dos desenquadramentos de percentual mínimo de garantias);
  - *Suitability*;
  - Supervisão de operações e de ofertas (registro das conclusões das análises);
  - Prevenção à lavagem de dinheiro; e

- Clubes de investimento.

- Diretórios que contenham informações relacionadas aos processos mencionados acima; e
- Canais de recebimento de ordens de clientes (exemplo: gravação de voz e mensageria).

Cabe destacar que as configurações das rotinas devem apresentar ao menos informações da periodicidade (*schedule*), identificação da informação e a origem e destino (exemplo: servidores e respectivos diretórios, mídias de *backup*, localidades).

Nota: Será considerado como *backup*, rotina de cópia de segurança de informações que permita recuperar informação íntegra, mesmo que haja um erro na produção, como deletar ou alterar um registro, a cópia permite recuperar os dados como estavam na época da cópia realizada. Exemplo de *backup*: mídias de *backup* (fitas DAT, mídias removíveis, *storages* e etc.). Métodos de espelhamento, sincronismo e/ou replicação de informações que em casos de alteração, deleção de um registro em produção, repliquem a mesma informação na cópia da informação e não permitem restaurar a informação antes do erro, não atendem ao requisito. Esses casos atendem ao processo de continuidade dos negócios (item 12.2 do Procedimento de Teste).

14.3) Análise da execução e monitoramento dos procedimentos de *backup*

Em amostra de 10 dias úteis, tendo como base o escopo de *backup* mapeado no procedimento anterior, avaliar se as rotinas de *backup* foram executadas todos os dias da amostra e para todo o escopo avaliado, mediante análise do *log* de execução ou evidência equivalente. Caso tenha falha ou não processamento do *backup* para a amostra avaliado, solicitar registro e tratamento do erro, conforme processo implantado pelo Participante. (Itens 47 e 48).

14.4) Análise da integridade dos *backups*

Tendo como base o processo de teste da integridade e da recuperação das informações dos *backups* definido pelo Participante (escopo, plano de testes, frequência), avaliar evidências de execução dos testes de restauração (item 49). Amostra: Testes mais recentes que em conjunto demonstrem restauração de todo escopo de sistemas/dados/ordens do *backup*.

14.5) Análise do armazenamento externo diário às instalações principais

Tendo como base o processo de armazenamento dos *backups* em local externo aos dados principais definido pelo Participante, avaliar se o local e/ou contrato de prestação de serviço (caso fornecido por terceiro) possui acesso controlado e controles de combate a incêndio (item 67). Adicionalmente, para amostra de 10 dias, avaliar se os *backups* foram armazenados, diariamente, em local externo aos dados principais (Item 50).

14.6) Análise da retenção dos *backups*

Avaliar se os *backup*s armazenados em local externo aos dados principais são retidos pelo período mínimo de 5 anos, ou desde a data de implementação do sistema. Evidências utilizadas para análise:

- Inventário das mídias de *backup* do Participante (item 51);
- Trilhas de auditoria dos registros de entrada/saída aos sistemas de negociação (item 7);
- Trilha de auditoria da rede corporativa e dos sistemas escopo (item 30); e
- Evidência de retenção de todo(s) o(s) canal(ais) de recebimento de ordens de clientes (exemplo: gravação de voz e mensageria) (item 61).

D. GERENCIAMENTO DE MUDANÇAS

15) Procedimento de Gerenciamento de Mudanças

Principal Requisito Normativo: Item 147 do Roteiro Básico.

Documentos utilizados na Execução do Procedimento de Teste:

- Item 52: Procedimento de gestão de mudança;
- Item 53: Lista de mudanças;
- Item 54: Diretórios de produção dos sistemas escopo; e
- Item 55: Documentação das mudanças.

Procedimento de Teste

15.1) Avaliação da suficiência do procedimento de gerenciamento de mudanças

Avaliar se os procedimentos documentados do gerenciamento das mudanças de *softwares*, hardware e infraestrutura (item 52) ou os controles mapeados no levantamento do processo de mudanças validado pelo Participante, definem, no mínimo, as seguintes diretrizes:

- Análise de impacto;
- Planejamento da execução;
- Roteiro e evidência de testes de homologação e de produção;
- Aprovação para implementação;
- Plano de retorno; e
- Documentação da mudança.

15.2) Relação de mudanças ocorridas no período escopo da auditoria

Receber inventário com todas as mudanças ocorridas nos sistemas que suportam os processos de negócio relacionados à B3 para o período escopo da auditoria (item 53), contendo no mínimo as seguintes informações:

- Identificação da mudança;

- Sistema envolvido;
- Descrição da mudança;
- Classificação da mudança (normal, emergencial e etc.);
- Data (abertura, homologação, aprovação, implementação, término e etc.); e
- Status da mudança.

15.3) Mapeamento das mudanças ocorridas no período escopo da auditoria

Mapear os diretórios de produção utilizados pelos sistemas que suportam os processos de negócio relacionados à B3 (item 54) e evidenciar as datas das últimas alterações realizadas em ambiente de produção, a partir da compilação dos arquivos (.exe, .dll, .ocx, .aspx, .htm e etc.) utilizados pelo sistema, contendo, no mínimo, as seguintes informações:

- Nome do diretório;
- Nome dos arquivos armazenados no diretório com a extensão;
- Data de criação e modificação dos arquivos; e
- Tamanho do arquivo.

15.4) Avaliação de amostra

Para amostra de 10 mudanças ocorridas desde a data da última auditoria, identificadas nos diretórios mapeados (item 54), avaliar a documentação de cada mudança (itens 53 e 55) quanto ao registro da mudança, análise de impacto, planejamento da execução, roteiros e execução de testes em ambiente segregado ao de produção, aprovação das áreas envolvidas antes da implementação em produção e criação de planos de retorno. Verificar se documentação enviada consta na lista de mudanças enviada pelo Participante. A documentação deve estar de acordo com os requisitos mínimos do Roteiro Básico e com o procedimento de Gerenciamento de Mudanças e/ou levantamento dos processos validado pelo Participante (item 52).

16) Segregação de Ambientes dos Sistemas Aplicativos

Principal Requisito Normativo: Item 148 do Roteiro Básico.

Documentos utilizados na Execução do Procedimento de Teste:

- Item 29: Planilha de sistemas; e
- Item 56: Segregação de ambientes.

Procedimento de Teste

16.1) Mapeamento da infraestrutura do Participante

Obter o mapeamento dos sistemas que suportam os processos de negócio relacionados à B3 (item 29) contendo, no mínimo, as seguintes informações:

- Nome do sistema;
- Data de implantação (mês/ano);
- Banco de dados;
- Sistema operacional do servidor que suporta o sistema;
- Ambiente de homologação para as camadas de aplicação e banco de dados;
- *Hostname* do servidor; e
- IP do servidor.

16.2) Segregação de ambientes nos sistemas aplicativos

Tendo como base a amostra das mudanças ocorridas (item 15.4 do Procedimento de Teste), avaliar se as evidências dos testes realizados identificam que os testes foram realizados em ambientes segregados ao ambiente de produção para as camadas de aplicação e de banco de dados.

Caso as evidências dos testes realizados sejam insuficientes, para os sistemas da amostra das mudanças ocorridas (item 15.4 do Procedimento de Teste), avaliar se possuem

ambientes segregados ao de produção para as camadas de aplicação e de banco de dados, como *prints* de tela dos ambientes mencionados (item 56).

17) Atualizações de Segurança - Sistema Operacional

Principal Requisito Normativo: Item 149 do Roteiro Básico.

Documentos utilizados na Execução do Procedimento de Teste:

- Item 57: Atualizações dos sistemas operacionais.

Procedimento de Teste

17.1) Suficiência do processo implementado pelo Participante para atualização do Sistema Operacional

Mapear o processo de atualizações técnicas e de segurança do sistema operacional Windows definido pelo Participante, e avaliar se são realizados testes para verificação de compatibilidade, antes da atualização no parque de estações de trabalho/servidores do Participante.

Nota: O procedimento para verificação de compatibilidade das atualizações técnicas e de segurança deve abranger todas as versões de sistemas operacionais Windows utilizadas pelo Participante em ambiente de produção.

17.2) Relação de atualizações críticas de segurança disponibilizadas pelo fornecedor

Extrair diretamente do site do fornecedor (Microsoft) do sistema operacional *Windows*, a relação de atualizações críticas (incluindo atualizações de segurança), que foram disponibilizadas desde a última auditoria realizada.

17.3) Avaliação de amostra

Para amostra de 10 estações de trabalho e 5 servidores, coletar evidências das atualizações instaladas/pendentes dos sistemas operacionais *Windows*, das seguintes formas:

- Execução do comando: wmic qfe list full >nomedoarquivo.txt;
- Captura de tela do status de atualização da ferramenta *Windows Update*; ou

Avaliar se existem atualizações críticas (incluindo atualizações de segurança) pendentes de instalação em cada estação de trabalho e servidor da amostra, tendo como base a relação de atualizações disponibilizadas pelo fornecedor (item 17.2 do Procedimento de Teste).

Extrair relatório da ferramenta de gerenciamento, como WSUS, SCCM ou proprietária do Participante (se aplicável), contendo o status de atualização da ferramenta (item 57) e comparar com resultado obtido na amostra selecionada.

E. SUPORTE À INFRAESTRUTURA

18) Canais de Recebimento de Ordens

Principais Requisitos Normativos: Itens 150, 151 e 152 do Roteiro Básico

Documentos utilizados na Execução do Procedimento de Teste:

- Item 1: Lista de colaboradores ativos
- Item 3: Lista de Agentes Autônomos de Investimentos
- Item 29: Planilha de sistemas
- Item 58: Lista de ramais gravados – voz
- Item 60: Integridade e totalidade dos canais de recebimento de ordens
- Item 61: Retenção dos canais de recebimento de ordens
- Item 62: Inventário de gravação de voz
- Item 63: Manutenção do sistema de gravação de voz
- Item 65: Teste de gravação de voz *in loco*
- Item 66: Planilha de serviços de TI
- Item 67: Cópia dos contratos estabelecidos com os fornecedores de TI
- Item 72: Registros de indisponibilidade de sistemas
- Item 73: Regras e Parâmetros de Atuação
- Item 74: Escopo de gravação- mensageria
- Item 75: Monitoração dos canais de recebimento de ordens
- Item 76: Recuperação de e-mail.

Procedimento de Teste

18.1) Definição do escopo

Verificar na planilha de sistemas (item 29), no documento de Regras e Parâmetros de Atuação (item 73) e alinhar junto ao Participante quais as ferramentas de mensageria (incluindo correio eletrônico) e voz são utilizadas para o recebimento de ordens de clientes.

18.2) Manutenção das ferramentas de recebimento de ordens

Avaliar o procedimento do Participante para realizar a manutenção de cada canal de recebimento de ordens de clientes e solicitar o último relatório de manutenção (item 63). Para os cenários em que a manutenção do sistema e guarda de informações seja realizada por terceiros, analisar o contrato junto ao fornecedor responsável (itens 66 e 67), verificando cláusulas de níveis de serviço (SLA), confidencialidade, vigência e aprovações.

18.3) Integridade e totalidade

Realizar *walkthrough* de cada sistema de gravação de ordens de clientes (item 60) e verificar possibilidade de edição das informações e conteúdo mínimo (data, horário, remetente, destinatário e mensagem/gravação) sem registro da alteração.

18.4) Recuperação de e-mail

Realizar *walkthrough* para avaliar a recuperação de e-mail (item 76):

- Enviar e-mail de teste
- Excluir e-mail de teste da “Caixa de Entrada”
- Excluir e-mail de teste da caixa de “Mensagens Excluídas” ou por meio do comando “Shift+Del”
- Excluir e-mail de teste da pasta “Recuperar Itens Excluídos”
- Verificar o processo de recuperação de e-mail.

18.5) Retenção

Verificar se a retenção das ordens de clientes nos canais de recebimento de ordens (item 61) atende ao requisito de 5 anos ou desde a data de implantação, conforme informado na planilha de sistemas (item 29).

18.6) Escopo de gravação

Confrontar todos os operadores (itens 1 e 3 e mapeamento da mesa, custódia e escritórios de agentes autônomos de investimento realizado pela equipe de auditoria de negócios) que recebem ordens de clientes com o escopo de gravação das ferramentas de mensageria (item 74) e voz (item 58).

18.7) Monitoração contínua dos canais de recebimento de ordens e registros de indisponibilidade

Realizar *walkthrough* para verificar monitoração contínua dos canais de recebimento de ordens (item 75) a fim de identificar indisponibilidade no sistema ou ramal para o período auditado (item 72). Caso um prestador de serviço seja responsável pela monitoração, analisar o contrato junto ao fornecedor responsável (item 67), verificando cláusulas de níveis de serviço (SLA), vigência e aprovações.

18.8) Processo de gravação de voz

Realizar ligação de teste para 5 ramais da mesa de operações e/ou custódia (item 65) e verificar se o sistema realizou as gravações de voz e de forma íntegra e com qualidade.

18.9) Inventário de gravação de voz

Confrontar o inventário de gravações de voz (item 62) com as gravações por voz recebidas para atender a amostra de ordens selecionadas pela equipe de negócios. Verificar se as gravações constam no inventário de gravação de voz (data, hora, destino, origem, duração, diálogo e código) e selecionar, no mínimo, 5 gravações para extração do sistema de gravação de voz in loco e confrontar se a gravação apresentada consta no sistema e no inventário de gravação de voz (data, hora, destino, origem, duração, diálogo e código) e se possui o mesmo conteúdo da gravação apresentada.

Caso tenha algum tipo de divergência entre a gravação apresentada e o inventário de gravação de voz ou a gravação verificada *in loco* do sistema de gravação de voz, aumentar amostra para 100% do canal com divergência, como por exemplo, mesa de operações, escritório de agente de autônomo de investimento. Para ordens apresentadas por escrito (ferramentas de mensageria, incluindo e-mail), comparar para uma amostra, de no mínimo 5 ordens, a ordem recebida com a extração *in loco* na base de dados das gravações de ordens recebidas por ferramentas de mensageria. Em caso de divergência entre a ordem apresentada e a ordem extraída in loco, aumentar amostra conforme critério citado acima.

19) Contratos

Principal Requisito Normativo: Item 153 do Roteiro Básico

Documentos utilizados na Execução do Procedimento de Teste:

- Item 66: Planilha de serviços de TI
- Item 67: Cópia dos contratos estabelecidos com os fornecedores de TI

Procedimento de Teste

19.1) Definição do escopo

Prestadores de serviços mapeados no levantamento dos serviços de TI - planilha de serviços de TI (item 66) e os identificados durante a auditoria que não constem na planilha de serviços.

19.2) Avaliação dos contratos

Solicitar os contratos dos fornecedores (item 67) mapeados (item 66) e identificados durante auditoria e verificar se os documentos contemplam as seguintes cláusulas (quando aplicáveis):

- Aprovações (de ambas as partes)
- Vigência
- Objeto do contrato
- Níveis de serviço mínimo (SLA - *Service Level Agreement*), aplicável nos casos em que os serviços prestados afetem a disponibilidade dos serviços e compromisso com seus clientes, como fornecedores de:
  - Links de Dados (RCB, RCCF e lan-to-lan - Matriz, filais e contingência);
  - Sistemas de negociação (DMA I) cuja manutenção é realizada pelo prestador de serviços;
  - Sistemas de negociação (DMA II);
  - Custódia de informações;

  - Suporte de Informática e bancos de dados; e

- Confidencialidade das informações, aplicável nos casos de fornecedores que tenham acesso a informações críticas, como Canais de recebimentos de ordens, em que as informações sejam mantidas no fornecedor ou caso o fornecedor tenha acesso as informações no Participante;

  - Sistemas de negociação (DMA I) caso o fornecedor tenha acesso as informações no Participante;

  - Sistemas de negociação (DMA II);

  - Custódia de informações; e

  - Suporte de Informática e bancos de dados; e

20) Inventário de *Hardware* e *Software*

Principal Requisito Normativo: Item 154 do Roteiro Básico

Documentos utilizados na Execução do Procedimento de Teste:

- Item 68: Inventário de *softwares* homologados, *hardwares* e de licenças adquiridas
- Item 69: Amostra - Bloqueio para instalar software nas estações de trabalho.
- Item 79: Monitoramento dos Softwares não homologados – resultado do confronto dos softwares homologados com os softwares instalados

Procedimento de Teste

20.1) Avaliar suficiência do processo

No levantamento dos processos identificar se o Participante implantou processo de homologação de *software* e *hardware* antes de instalar em estações de trabalho e servidores. Além disso, identificar se o Participante implantou controles que inibam a instalação de *softwares* não homologados/maliciosos pelo Participantes e/ou controles que detectem instalação de *software* não homologados, para tratamento do evento. Solicitar inventário de *softwares* e *hardwares* homologados e de licenças adquiridas (item 68).

20.2) Teste de amostragem

Caso o Participante tenha implantado procedimento para inibir a instalação de softwares não homologados/maliciosos, como por exemplo, por meio da restrição da permissão de administrador da máquina (usuário local) para parte dos colaboradores, testar amostra de 10 estações de trabalho (item 69) e verificar se possuem permissão de instalação de *softwares* na máquina.

20.3) Monitoramento de *Softwares* Instalados x Softwares homologados

Caso o controle implantado para identificar instalação de software não homologado/malicioso seja apenas detectivo, como monitoramento dos softwares instalados em relação aos softwares homologados, solicitar evidência do monitoramento, do último resultado e dos planos de ação, caso aplicável (item 79). A expectativa da frequência do controle para identificar instalação de software não homologados é, no mínimo, semestral.

Caso o monitoramento de instalação de *softwares* não homologados no parque informatizado seja realizado em tempo real, verificar se a ferramenta possui configuração de alerta ativa e solicitar o último exemplo de alerta recebido e o registro do tratamento / plano de ação.

21) Antivírus

Principal Requisito Normativo: Item 155 do Roteiro Básico

Documento utilizado na Execução do Procedimento de Teste:

- Item 70: Antivírus instalado nas estações de trabalho e servidores.

Procedimento de Teste

21.1) Teste de amostragem - Antivírus

Identificar se há antivírus instalado e atualizado (com base na avaliação da data da vacina disponibilizada pelo fornecedor do antivírus na data do teste) na amostra de 10 estações de trabalho e 5 servidores selecionados para teste (item 70) ou se há procedimentos aplicados que forneçam segurança equivalente.

F. AGENTES AUTONOMOS DE INVESTIMENTO

22) Agentes Autônomos de Investimentos

Principais Requisitos Normativos: Itens 35, 37, 51, 144, 145, 151 e 152 do Roteiro Básico

Documentos utilizados na Execução do Procedimento de Teste:

- Item 3: Relação de Agentes Autônomos de Investimento
- Item 11: Lista das estações de trabalho
- Item 14: Intervalo de endereço IP (*Internet Protocol*)
- Item 46: Agendamento das rotinas de *backup*
- Item 47: Log de execução dos *backups*
- Item 48: Plano de ação das falhas na execução dos *backup*s
- Item 50: Armazenamento externo de *backup*
- Item 60: Controles de integridade e totalidade dos canais de recebimento de ordens
- Item 61: Evidência de retenção das ordens de clientes nos canais de recebimento de ordens
- Item 62: Registro das gravações
- Item 75: Monitoração do sistema de gravação de voz
- Item 76: Controles de integridade e totalidade do correio eletrônico.

Procedimento de Teste

22.1) Mapeamento da infraestrutura

Tendo como base o(s) escritório(s) de AAI visitado(s) (item 3), realizar mapeamento da(s) estação(ões) de trabalho dos profissionais alocados na mesa de operações e identificar os seguintes aspectos (itens 11 e 14):

- Identificação da máquina (*Hostname*)

- Nome completo do usuário (exemplo: João do Santos)
- Sistema(s) de negociação e usuário(s) utilizado(s) por cada operador
- Canal(is) de recebimento de ordens de clientes (gravação de voz, e-mail e etc.) e usuário(s) utilizado(s) por cada operador
- Endereço IP (*Internet Protocol*) interno e externo da estação de trabalho.

Avaliar se o escritório dispõe de sala(s) de clientes e se existe(m) estação(ões) de trabalho para uso de cliente(s). Adicionalmente, mapear a(s) estação(ões) de trabalho conforme acima, caso exista(m).

22.2) Análise do escopo e da frequência da configuração do *backup*

Mapear se o procedimento de *backup* do(s) canal(ais) de recebimento de ordens de clientes no(s) escritório(s) de AAI é realizado pelo próprio AAI ou pelo Participante.

Seguir os passos e testes do item 14.2 descritos no documento que define os testes de *backup* “Execução, monitoramento e armazenamento externo de cópias de segurança (*backups*)”.

22.3) Análise da execução e monitoramento do *backup*

Seguir os passos e testes do item 14.3 descritos no documento que define os testes de *backup* “Execução, monitoramento e armazenamento externo de cópias de segurança (*backups*)”.

22.4) Análise da integridade dos *backups*

Seguir os passos e testes do item 14.4 descritos no documento que define os testes de *backup* “Execução, monitoramento e armazenamento externo de cópias de segurança (*backups*)”.

22.5) Análise do armazenamento externo diário às instalações principais

Seguir os passos e testes do item 14.5 descritos no documento que define os testes de *backup* “Execução, monitoramento e armazenamento externo de cópias de segurança (*backups*)”.

22.6) Retenção das ordens de clientes

Seguir os passos e testes do item 14.6 descritos no documento que define os testes de *backup* “Execução, monitoramento e armazenamento externo de cópias de segurança (*backups*)”.

22.7) Monitoramento do(s) canal(ais) de recebimento de ordens de clientes

Mapear se o monitoramento do(s) canal(ais) de recebimento de ordens de clientes no(s) escritório(s) de AAI é realizado pelo próprio AAI ou pelo Participante.

Seguir os passos e testes do item 18.7 descritos no documento que define os testes dos “Canais de Recebimento de Ordens”.

22.8) Controle de integridade das gravações de ordens

Avaliar se as ferramentas de gravação de voz e mensageria (item 62) possuem inventário de gravação, e se possuem as seguintes informações registradas:

- Data
- Horário de início
- Horário de fim ou duração
- Telefone/ramal de origem
- Telefone/ramal de destino
- Identificação do telefone/ramal de origem e de destino (quando sistema de gravação de voz)
- Identificação do usuário de origem e de destino (quando sistema de mensageria)
- Código da gravação.

Adicionalmente, para cada um do(s) canal(ais) de recebimento de ordens de clientes, seguir os passos do item 18.3, 18.4 e 18.9 descritos no documento que define os testes dos “Canais de recebimento de ordens”.

Mensageria e gravação de voz (item 60):

Mapear se a contratação e gestão do(s) canal(ais) de recebimento de ordens de clientes no(s) escritório(s) de AAI são realizadas pelo próprio AAI ou pelo Participante.

A partir da ferramenta de gerenciamento de cada canal de recebimento de ordens de clientes, avaliar a possibilidade de:

- Inclusão, alteração e exclusão das mensagens recebidas por mensageria
- Inclusão, alteração e exclusão dos arquivos de áudio do sistema de gravação de voz.

Mensageria - e-mail (item 76):

- Enviar e-mail de teste;
- Excluir e-mail de teste da “Caixa de Entrada” e da caixa “Mensagens Excluídas”, por meio do comando “Shift+Del”;
- Excluir e-mail de teste da pasta “Recuperar Itens Excluídos”.
- Verificar o processo de recuperação de e-mail.

Adicionalmente, avaliar se o(s) canal(ais) de recebimento de ordens possuem trilha de auditoria que identifique exclusões e/ou alterações realizadas pelos usuários.

G. CONTROLES INTERNOS

23) Relatórios de Controles Internos

Principais Requisitos Normativos: Item 117 do Roteiro Básico e ICVM 505/2011 (Artigo 3º e 4º)

Documentos utilizados na Execução do Procedimento de Teste:

- Relatórios de controles internos (solicitação de negócios)

Procedimento de Teste

23.1) Análise dos relatórios

i) Com base nos 2 últimos relatórios de controles internos semestrais emitidos pelo Participante, verificar:

a) Se os relatórios foram emitidos pelos Diretor de Controles Internos;

b) Se os relatórios foram enviados formalmente aos órgãos de administração.

Os documentos apresentados pelo Participantes que não chegaram ao público alvo, não serão considerados para atender a esse requisito, visto que o foco do requisito é o reporte para a alta administração da instituição da avaliação dos controles internos.

O foco da avaliação da BSM é verificar se os relatórios ou outros documentos complementares que chegam ao público alvo descrito acima, detalham as seguintes informações para o escopo do requisito 117 do Roteiro Básico:

i) Descrição dos exames efetuados para avaliá-los: procedimento do teste e da abrangência do teste (exemplo: Parâmetros de senha: quais sistemas foram avaliados (universo), período de análise, qual análise realizada, quais parâmetros foram avaliados, qual resultado do teste esperado). Nesse passo as informações dos exames efetuados devem ser suficientes para que possam ser executados novamente e chegar ao mesmo resultado.

Caso o escopo de avaliação não seja completo, detalhar no relatório o critério do escopo avaliado e a estratégia de avaliação.

ii) Descrição dos resultados e conclusões dos exames efetuados: Detalhar o resultado dos testes. O que falhou (exemplo: qual sistema, qual parâmetro, qual conclusão).

iii) Descrição das não conformidades formalmente identificadas pela própria instituição e também pelos seus reguladores e autorreguladores. Nessa etapa avaliaremos se o relatório de controles internos aborda os apontamentos identificados pela BSM e pelo Participante.

iv) Descrição das recomendações a respeito das não conformidades identificadas acima (item iii), com a descrição do plano de ação, quando aplicável. Plano de ação deve detalhar a ação efetuada, o prazo e o responsável pelo plano de ação.

v) Descrição do acompanhamento da implementação dos planos de ação propostos no relatório atual e nos relatórios anteriores em aberto, bem como da eficácia das medidas corretivas e dos planos de ação implantados, sobretudo para evitar recorrências de não conformidades

vi) Em casos de não cumprimento de plano de ação estabelecidos em relatórios anteriores: como atraso, mudança de plano, ou outras situações, descrever os motivos e os próximos passos.

Os itens (i) a (vi) requeridos para o relatório de controles internos podem estar contidos em relatórios equivalentes, como, por exemplo, relatório de auditoria interna e relatório de controles internos do conglomerado do Participante, desde que tenham sido emitidos e encaminhados formalmente aos órgãos de administração do Participante e/ou do seu conglomerado.

A avaliação do ambiente de controles internos pode ser terceirizada, mas a avaliação deve ser independente dos resultados da BSM e dos reguladores.

O relatório semestral de avaliação de controles internos deve abranger, no mínimo, os seguintes aspectos e sua conformidade com a legislação e a regulamentação vigentes:

i) monitoração da adequação da recomendação de produtos, serviços e operações ao Perfil de Investimento do Cliente e das operações realizadas em nome de Clientes em relação aos respectivos Perfis de Investimento (*suitability*);

ii) avaliação dos controles relacionados aos processos de recepção e de execução de Ordens, cadastro de Clientes, de gestão de riscos, de custódia, de liquidação e de movimentação de conta-corrente e de conta-corrente gráfica;

iii) monitoração da conformidade dos procedimentos executados pelo Participante em relação às suas Regras e Parâmetros de Atuação, em especial quanto à atuação de pessoas vinculadas e à carteira própria;

iv) avaliação da segregação das funções desempenhadas pelos integrantes do Participante, de forma que seja evitado o Conflito de Interesses;

v) monitoração das operações e das ofertas;

vi) monitoração da atuação de profissionais de operações (inclusive estagiários que desempenhem tal função), Agentes Autônomos de Investimento e de profissionais terceirizados vinculados ao Participante, inclusive daqueles que estejam em ambiente físico externo;

vii) monitoração da existência e da validade da certificação dos profissionais que atuarem nos mercados da B3;

viii) prevenção e detecção de lavagem de dinheiro;

ix) segurança das informações: gerenciamento de acessos e senhas (redes, sistemas e bancos de dados, incluindo Canal de Relacionamento Eletrônico com o Cliente) e identificação dos sistemas sem Trilhas de Auditoria;

x) continuidade dos negócios: acompanhamento e avaliação das atualizações e dos resultados dos testes em relação aos objetivos estabelecidos;

xi) registro das situações de indisponibilidade em sistemas que impactem as operações dos Clientes (sistemas de negociação) e a gravação das Ordens dos Clientes;

xii) monitoração, identificação e registro de situações de ameaças à rede interna de computadores, aos sistemas e aos dados que contenham informações dos Clientes mantidas sob sua guarda; e

xiii) monitoração da implementação de Política de Responsabilidade Socioambiental.

24) Recorrência de apontamentos de auditoria

Principais Requisitos Normativos: Item 118 do Roteiro Básico e ICVM 505/2011 (Artigo 3º e 4º)

Documentos utilizados na Execução do Procedimento de Teste:

- Relatórios de auditoria da BSM da auditoria em curso e de planos de trabalhos anteriores;
- Respostas dos relatórios emitidos nas auditorias anteriores enviadas pelo Participante;
- Ofícios com determinações e recomendações emitidos pela BSM.
- Relatório de controles internos emitidos pelo Participante.

Procedimento de Teste

24.1) Análise da recorrência de apontamentos

Avaliar se os apontamentos críticos identificados na auditoria em curso são recorrentes quando comparados aos relatórios da BSM de planos de trabalhos anteriores e se as falhas não diminuem ou não se resolvem com o tempo, em desacordo com o plano de ação informado pelo Participante.

Na análise de recorrência de apontamentos, são considerados:

- Não cumprimento do Plano de Ação informado na resposta do Participante ao relatório de auditoria da BSM do(s) ano(s) anterior(es), isto é: (i) não correção das situações identificadas nas auditorias anteriores e/ou (ii) não implementação das melhorias e dos planos de ação informados pelo Participante.
- Ineficácia na implementação de Plano de Ação, isto é, o plano de ação foi implantado, mas não evita a recorrência das falhas apontadas nas auditorias anteriores na auditoria em curso.
- Os itens são agravados em casos de não cumprimento de planos de ação ou plano de ação ineficaz referentes a apontamentos que a BSM recomendou ou determinou para não haver recorrência.

- Além disso, comparamos o resultado desses apontamentos recorrentes ou com implantação ineficaz com o relatório de controles internos (2 últimos) emitidos pelo Participante.

Os testes descritos nesse documento foram elaborados tento como referência a base legal e regulamentar vigente e framework e boas práticas de mercado: ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27032, CobiT (Control Objectives for Information and related Technology) e ITIL (Information Technology Infrasructure Library).