Manual de Segurança Cibernética

Elaboração: *Compliance*, Sistemas e Tecnologia

Aprovação: Diretoria

Versão: 2

Código: M044

Vigente Desde: 04/2019

Última Versão: 08/2020

ÍNDICE

1. OBJETIVO

Este documento estabelece as diretrizes relacionadas à segurança cibernética do Grupo BR Partners.

2. APLICABILIDADE

Os dispositivos deste documento são aplicáveis a todas as empresas do Grupo BR Partners, colaboradores, parceiros de negócios, fornecedores e prestadores de serviços, que atuem nos ambientes físicos e/ou tecnológicos para processar dados sensíveis controlados e/ou pertencentes ao Grupo BR Partners.

3. RESPONSABILIDADES

3.1. Colaboradores

- Participar ativamente dos programas de disseminação da cultura de segurança cibernética; e
- Respeitar e aderir a todos os preceitos estabelecidos nos documentos relacionados à segurança cibernética.

3.2. *Compliance*

- Manter atualizado o mapeamento de requisitos regulatórios, para fins de fiscalização dos processos e procedimentos corporativos;
- Receber das áreas responsáveis e tabular os níveis de aderência aos controles de segurança cibernética;
- Apoiar a área de Segurança da Informação na gestão de controles de riscos à segurança cibernética;
- Atuar nos trabalhos de gestão da continuidade de negócios; e
- Participar do comitê de Riscos e *Compliance* para tratar de assuntos relacionados à segurança cibernética.

3.3. Jurídico

A área Jurídica é responsável por:

- Gerir os modelos de contratos com fornecedores e prestadores de serviço, mantendo atualizadas cláusulas regulatórias relacionadas à segurança cibernética, prevendo direito de realização de trabalhos de *due dilligence*.

3.4. Recursos Humanos

A área de Recursos Humanos é responsável por:

- Promover e apoiar as áreas envolvidas na construção e gestão do programa de conscientização e capacitação em segurança cibernética, operacionalizando eventos e tabulando resultados de avaliação de absorção do conhecimento;
- Realizar a gestão da absorção do conhecimento, apontando aos gestores departamentais correspondentes e demais interessados a curva de absorção do conhecimento ministrado, recomendando reciclagens ou eventos adicionais, caso, em conjunto com o *Compliance*, entenda ser necessário; e
- Operacionalizar todos os trabalhos relacionados ao programa de conscientização e capacitação em segurança cibernética.

3.5. Riscos

A área de Riscos é responsável por:

- Conhecer detalhadamente os processos e riscos envolvidos nas operações da instituição;
- Documentar e armazenar os eventos de perda relacionados aos incidentes de segurança cibernética;
- Mapear potenciais perdas devido a processos, multas e demais incidentes relativos à segurança cibernética;
- Divulgar os relatórios em seus respectivos prazos;
- Convocar e/ou participar dos respectivos comitês;
- Disseminar conhecimento sobre Riscos; e
- Monitorar os processos e controles de Riscos que lhe são atribuídos.

3.6. Segurança da Informação

Os colaboradores são responsáveis por:

- Promover ativamente os trabalhos de análise e avaliação de riscos à segurança cibernética, produzindo relatórios técnicos e executivos, remetendo-os à Diretoria e demais interessados;
- Manter as áreas de TI, Sistemas e *Compliance* envolvidas nos trabalhos de análise e avaliação de riscos à segurança cibernética, validando junto a estas quaisquer questões relacionadas;
- Atuar nos trabalhos de gestão da continuidade de negócios;
- Receber das áreas de TI e Sistemas relatórios técnicos relacionados aos trabalhos de detecção e mitigação de vulnerabilidades tecnológicas em sistemas corporativos, utilizando estas informações para gerenciar os controles (*KRI's*), relacionados aos riscos à segurança cibernética;
- Realizar a classificação da informação e de dados;
- Trabalhar em conjunto com as áreas de Tecnologia, Sistemas, *Compliance* e

Negócios (quando aplicável), na contratação de serviços de segurança dos dados e segurança cibernética;
- Realizar a gestão da rastreabilidade de informações críticas ao negócio, especialmente daquelas classificadas como sensíveis;
- Definir os parâmetros a serem utilizados na avaliação da relevância dos incidentes de segurança cibernética;
- Elaborar controles pertinentes e verificar aderência a novas leis, normas e boas práticas, mantendo-os atualizados e em nível de eficácia;
- Participar do comitê de Riscos e *Compliance* para tratar de assuntos relacionados à segurança cibernética;
- Apoiar trabalhos de *due dilligence* relacionados à segurança cibernética (dados, informação, ambientes, outros) de prestadores de serviço e fornecedores;
- Gerenciar trabalhos de disseminação da cultura de segurança cibernética, realizados junto a colaboradores do Grupo BR Partners, prestadores de serviço e fornecedores contratados;
- Gerenciar trabalhos de capacitação em defesa cibernética voltados aos colaboradores de SI (Segurança da Informação); e
- Direcionar às áreas de Tecnologia da Informação, Sistemas e *Compliance* quaisquer necessidades relacionadas à segurança cibernética;
- Avaliar os incidentes de segurança da informação trazendo a sua amplitude e magnitude do incidente, nível de severidade e nível de prioridade; e
- Registrar todas as informações pertinente para investigação e tratamento do incidente para acionar os principais envolvidos que irá atuar no processo de resposta a incidente de segurança da informação;

3.7. Sistemas

Os colaboradores são responsáveis por:

- Apoiar os trabalhos de gestão do catálogo de ativos de TI, fornecendo informações atualizadas concernentes aos sistemas corporativos do Grupo BR Partners;
- Apoiar ativamente os trabalhos de análise e avaliação de riscos à segurança cibernética;
- Apoiar ativamente os trabalhos de identificação e correção de vulnerabilidades tecnológicas, relacionadas aos sistemas corporativos;
- Promover em tempo hábil quaisquer correções necessárias aos sistemas corporativos, apontados em relatório periódico de testes e identificação de vulnerabilidades (*pentests*);
- Garantir disponibilidade dos recursos de registros de atividades e acessos (logs) em todos os sistemas corporativos, promovendo sua rastreabilidade;
- Garantir que todos os sistemas críticos ao negócio (ou que contenham dados sensíveis) possuam recursos de criptografia e segregação de acessos;

- Envolver-se ativamente nos trabalhos de gestão da continuidade de negócios, sempre que necessário ou solicitado;
- Participar do comitê de Riscos e *Compliance* para tratar de assuntos relacionados à segurança cibernética; e
- Apoiar trabalhos de disseminação da cultura de segurança cibernética, realizados junto a colaboradores do Grupo BR Partners, de prestadores de serviço e fornecedores contratados.

3.8. Tecnologia da Informação

A área de Tecnologia da Informação é responsável por:

- Tratar as vulnerabilidades ou ameaças cibernéticas potenciais identificadas para cada ativo tecnológico da corporação;
- Gerenciar trabalhos de mitigação ou eliminação das vulnerabilidades cibernéticas mais graves, identificadas através dos trabalhos de análise e avaliação de riscos à segurança cibernética;
- Apoiar os trabalhos de análise e avaliação de riscos à segurança cibernética e de classificação da informação e de dados encabeçados pela área de Segurança da Informação;
- Gerir sistemas de registro na camada de infraestrutura (alinhados ao nível da classificação do ativo de TI e dados contidos) preservando seus registros (logs), promovendo a rastreabilidade;
- Gerir os acessos às informações corporativas (segregação de funções e controle de acessos) conforme parâmetros e controles previamente estabelecidos no tocante a *file server* ou sistemas de arquivo compatível;
- Apoiar os trabalhos periódicos de testes e varreduras para detecção de vulnerabilidades cibernéticas em sistemas (*pentests*);
- Participar do comitê de Riscos e *Compliance* para tratar de assuntos relacionados à segurança cibernética;
- Atuar nos trabalhos de gestão da continuidade de negócios, sempre que necessário ou solicitado;
- Apoiar trabalhos de *due dilligence* relacionados aos aspectos tecnológicos (dados, informação, ambientes, outros) de prestadores de serviço e fornecedores; e
- Apoiar trabalhos de disseminação da cultura de segurança cibernética, realizados junto a colaboradores do Grupo BR Partners, de prestadores de serviço e fornecedores contratados.

4. DESCRIÇÃO DA NORMA

4.1. Considerações Gerais

Os integrantes da alta administração do Grupo BR Partners, representados pelos membros do Comitê de Gestão do Grupo BR Partners, servem de exemplo para todos os colaboradores, fornecedores e parceiros, ratificando apoio irrestrito às práticas estabelecidas neste documento.

A alta administração do Grupo BR Partners é composta pelos membros do Comitê de Gestão do Grupo BR Partners, os quais também são todos Diretores de sociedades integrantes do Grupo BR Partners e demonstram comprometimento com as práticas de segurança cibernética, na condução dos negócios de todo o Grupo BR Partners.

Esse comprometimento é evidenciado por meio da inserção de temas relacionados à segurança cibernética em pautas das reuniões de diretoria, sempre que necessário ou demandado. Também evidenciam seu comprometimento com a liberação anual de recursos financeiros necessários, destinados aos programas relacionados à segurança cibernética, previamente homologados e aprovados pelo *board* executivo.

4.2. Redução da Vulnerabilidade

Dependendo dos ativos de TI, a vulnerabilidade pode representar um maior ou menor risco para a organização, dependendo da importância do sistema ou ativo para a instituição.

As vulnerabilidades são classificadas por critérios de impacto aos ativos tecnológicos face à possibilidade de sua exploração. Esta classificação é dada por alto, médio e baixo impacto ao ativo. Os processos utilizados para a análise de vulnerabilidades são:

- Atualização do catálogo de ativos de TI, com atribuição de valores qualitativos de importância desse ativo (e de seus dados contidos) para o negócio (classificação);
- Identificação das vulnerabilidades ou ameaças potenciais para cada ativo tecnológico; e
- Mitigação ou eliminação das vulnerabilidades mais graves dos recursos mais valiosos.

No contexto da análise de vulnerabilidades, utilizam-se processos e ferramentas especializadas de reconhecida reputação nos mercados nacional e internacional para:

- Registro, monitoramento e análise (alinhado ao nível da classificação do ativo e dados contidos) das operações de acesso, preservando seus registros (logs), promovendo a rastreabilidade;
- Gestão dos acessos às informações (segregação de funções e controle de acessos), garantindo o correto tratamento e processamentos dos dados; e
- A realização periódica de testes e varreduras para detecção de vulnerabilidades em sistemas (*pentests*).

4.3. Rastreabilidade das Informações Sensíveis

Em alinhamento aos processos de classificação da informação (item 4.7) toda informação recebe uma classificação. As informações classificadas como 'sensíveis' ao negócio recebem níveis adicionais de proteção e rastreabilidade.

Todos os sistemas que tratam informação classificada como sensível mantém log de acessos de leitura, escrita e mudança são registrados nos concentradores de log com a trilha de auditoria para todos os acessos e tratamento da informação sensível.

Recursos tecnológicos como criptografia, concentrador de registros (logs) de rede (p.ex.: SIEM) com análise proativa e procedimentos de pronta-resposta a incidentes cibernéticos (com procedimentos aprovados pela alta direção), são adotados e continuamente geridos por pessoal específico e especializado, para estas informações classificas como sensíveis.

Estes controles, processos e procedimentos são aplicados e geridos pelas áreas de Tecnologia da Informação, Sistemas, Riscos e *Compliance*, garantindo a manutenção da segurança cibernética e mantendo os riscos cibernéticos sob controle.

4.4. Registro, Análise e Impacto de Incidentes Relevantes

Em seus relatórios de análise e avaliação de riscos cibernéticos, as áreas responsáveis registram todos os incidentes ocorridos dentro de um certo período e destacam aqueles considerados relevantes para as atividades do Grupo BR Partners (i.e.: com categorização de severidade com nível médio ou acima). Identifica quais controles de segurança sofreram agressão (o que possibilitou a concretização do incidente), suas causas e impactos aos processos de negócio do Grupo BR Partners.

Sugere também proposição de ações mitigatórias aos responsáveis, alinhados aos processos de gestão da continuidade de negócios, apontando os impactos mensurados aos ativos de TI que apoiam os processos de negócio.

Também, incluem estes incidentes destacados em seus trabalhos de elaboração de cenários para testes de incidentes cibernéticos (previstos pelo item 4.5).

4.5. Elaboração de Cenário de Incidentes

Consoante aos relatórios de avaliação e análise de riscos cibernéticos são propostos cenários de incidentes sobre os ativos considerados sensíveis ao negócio, alinhados aos processos críticos de negócio do Grupo BR Partners. O sistema de gestão de continuidade dos negócios (SGCN), do Grupo BR Partners, foi elaborado baseando-se nas melhores práticas de mercado e consideram-se os casos de uso de cenários de incidentes que periodicamente é revisto através do BIA (Análise de Impacto).

Em casos emergenciais os cenários de incidentes e a análise de impacto aos negócios para mitigação de riscos cibernéticos são registrados e apresentados a todos os

responsáveis, possibilitando alinhamento sobre o cenário atual de riscos e ações necessárias.

Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes cibernéticos, abrangem, inclusive, informações recebidas de empresas prestadoras de serviços e terceiros.

4.6. Prevenção de Incidentes de Terceiros

Pensando na integralidade dos níveis de segurança cibernética necessários aos dados categorizados como 'sensíveis' aos negócios do Grupo BR Partners, foram adotados processos e controles específicos voltados a prestadores de serviços, como seguem:

- Adoção de cláusulas contratuais que exigem uma gestão eficaz da segurança cibernética por parte de prestadores de serviços e terceiros que porventura precisem (por força de escopo de contrato) manusear dados ou informações categorizadas como sensíveis aos negócios do Grupo BR Partners;
- Exigência contratual de existência de Política de Segurança Cibernética e documentos correlatos, revisados e divulgados a seus próprios colaboradores em data recente;
- Adoção de cláusulas contratuais que garantam aos auditores (internos ou contratados para este fim) do Grupo BR Partners o direito à realização de diligências internas, com a finalidade de avaliar os níveis de segurança cibernética dispensados a dados sensíveis (pertencentes ou controlados pelo) do Grupo BR Partners, em seus ambientes tecnológicos; e
- Adoção de controles periódicos para avaliação do nível de segurança de dados e informações, praticados por empresas prestadoras de serviços, sob pena de rescisão contratual (unilateral e sem ônus à contratante) caso se comprove baixo nível (ou inferior aos praticados pelo Grupo BR Partners) de gestão de segurança da cibernética, especialmente os relacionados a dados sensíveis pertencentes (ou controlados) ao Grupo BR Partners. Seus programas de segurança cibernética e da informação devem contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela própria instituição.

4.7. Classificação de Dados

Durante os trabalhos de análise de vulnerabilidades, ativos tecnológicos são classificados quanto à sua importância ao negócio. Também, seus dados contidos recebem apropriada classificação, permitindo aplicação de recursos adicionais de segurança. Os níveis de classificação de dados (sempre sob a ótica do negócio) são: irrelevante, média relevância e alta relevância.

Periodicamente são reavaliadas e executadas todas as etapas do processo de análise de vulnerabilidades, revisando o catálogo de ativos, sua criticidade e sensibilidade ao negócio, a classificação do ativo tecnológico e dado contido, seus recursos e níveis de segurança, bem como testes de vulnerabilidade direcionados.

4.8. Definição dos Parâmetros para Relevância dos Incidentes

Durante a análise e avaliação de riscos cibernéticos, são adotados parâmetros qualitativos para determinação da relevância dos ativos e dados (ou potenciais incidentes) cibernéticos aos negócios do Grupo BR Partners.

Tabulação de ativos e sua importância aos processos de negócio do Grupo BR Partners, suas vulnerabilidades mapeadas e o impacto ao negócio (caso a vulnerabilidade seja explorada) são constantemente revisados por pessoal especializado.

Os sistemas de monitoramento e gestão dos ambientes críticos (ativos e dados), ao identificarem um incidente com classificação de criticidade e importância terão prioridade no seu tratamento; é criada WAR ROOM para o tratamento deste incidente por equipe multidisciplinar incluindo as áreas de negócio do Grupo BR Partners envolvidas no incidente.

4.9. Gerenciamento de Dispositivos Móveis

Para o tráfego de dados classificados como sensíveis ao ambiente externo a rede corporativa deve ser instalado no dispositivo móvel um sistema de gerenciamento permitindo o controle do equipamento externo ao Grupo BR Partners, permitindo:

- Exclusão remota do equipamento, deletando todo conteúdo;
- Alteração de senha;
- Implementação de políticas pré-definidas para proteção ao dado trafegado;
- Verificação de conformidade do dispositivo;
- Monitoramento dos dados trafegados por ferramenta CASB.

4.10. Antivírus

O software de antivírus deve ser obrigatoriamente instalado em todas as estações de trabalho e servidores do Grupo BR Partners, conforme diretrizes abaixo:

- Somente pode ser utilizado o antivírus homologado pela Tecnologia;
- O *software* de antivírus deve ser instalado em servidores ou dispositivos de borda que proporcionem comunicação com redes públicas ou externas;
- Devem ser executadas varreduras periódicas de *scan* contra vulnerabilidades nos servidores e estações de trabalho;

- Todas as estações de trabalho e servidores devem possuir o *software* de antivírus instalado, atualizado e em comunicação constante com servidor que controla as políticas, vacinas e versões de *software*;
- As vacinas devem ser atualizadas diariamente, e *patches* de correção serão aplicados conforme GMUD agendada ou via criticidade através de incidente atrelado;
- O *software* de antivírus deve garantir a proteção do ambiente contra ataques de vírus nas estações de trabalho e servidores que fazem parte ou estejam conectados à rede corporativa;
- O *software* de antivírus deve ter como características: (i) detectar e eliminar vírus; (ii) limpar, mover ou apagar arquivos infectados; (iii) detectar, analisar e reparar arquivos contaminados por vírus, quando acessados, modificados ou criados; (iv) identificar vírus mesmo que estejam escondidos sob camadas de arquivos compactados, em anexo de e-mails e em todos os formatos utilizados; (v) permitir navegação na Internet com segurança, detectando e removendo perigosas formas de ataque via Internet; (vi) permitir isolamento de arquivos infectados em uma área segura da própria estação de trabalho ou servidor até que possam ser reparados, garantindo que outros arquivos não sejam contaminados; e
- Bloquear a opção que permite que os serviços do *software* de antivírus não sejam iniciados ou parados. A alteração de parâmetros do antivírus deve ser permitida apenas para as equipes responsáveis pela administração e operação deste serviço. Configurar senha de desinstalação no *software* de antivírus para que o usuário não possa desinstalar o mesmo.

Todas as exceções devem ser autorizadas pelas áreas de Tecnologia e de *Compliance*.

4.11. *Firewall*

O Firewall deve ser instalado em cada conexão da Internet e entre qualquer zona desmilitarizada (DMZ) e a zona interna da rede, bem como qualquer rede WAN contratada em provedores de serviço no Brasil e no exterior.

São restritos os acessos de entrada e de saída ao que é necessário para as áreas sensíveis, bem como rejeitado especificadamente os outros tráfegos.

Todos os firewalls de borda externa devem possuir obrigatoriamente sistema IPS (*Intrusion Prevention System*) instalado.

O processo de "Clean-up" envolvendo regras e objetos do firewall deve ser realizado a cada 3 (três) meses, caso aplicável.

O tráfego de Internet é monitorado via inspeção de pacotes e categorização de sites.

As documentações de Tecnologia referente a *Firewalls* devem possuir a descrição dos grupos e as responsabilidades de cada equipe envolvida, onde todos os envolvidos devem ter conhecimento e ciência das regras em funcionamento que estão sob sua responsabilidade, como por exemplo: portas liberadas, VPN's estabelecidas e demais recursos pré-estabelecidos devido a demanda de aplicação ou sistema.

As novas atribuições à *firewalls* devem ser feitas formalmente e com a aprovação da gerência de Segurança da Informação ou Comitê de Riscos e *Compliance*.

4.12. Inventário

O sistema de Inventário cataloga as informações de todos os *softwares* instalados nas estações de trabalho, conforme as seguintes características:

- Informações detalhadas do *software* instalado contendo versão, fabricante e data de instalação do mesmo;
- *Hardware* instalado no momento do inventário;
- Permitir segmentação de inventário por área;
- Versionamento do inventário realizado, permitindo revisões e comparações entre perfis;
- Processos em execução no momento da coleta dos dados;
- Conter relatórios gerenciais; e
- Possibilidade para exportação em formato texto e integração sistêmica.

4.13. Atualizações de Segurança de Estações de Trabalho e Servidores

As estações de trabalho e servidores devem ser atualizadas quanto aos *patches* de segurança e *bugs.*

É adotada uma ferramenta de distribuição de *patches* de segurança de forma automática como WSUS ou *System Center*. A periodicidade mínima de atualizações é a seguinte:

- Estações de Trabalho: no mínimo a cada 3 (três) meses ou necessidade urgente devido a incidente de segurança no *software* reportado pelo fabricante, sob avaliação; e
- Servidores: no mínimo anualmente ou necessidade urgente devido a incidente de segurança no *software* reportado pelo fabricante, sob avaliação.

4.14. Prevenção a Perda de Dados (DLP)

As ferramentas de prevenção a perda de dados (DLP – *Data Loss Prevention*), atuam no bloqueio de dispositivos USB e CD/DVD, impedindo gravação ou de forma parcial a realização de auditoria dos dados gravados nestes dispositivos.

Caso existam dados classificados como passíveis de bloqueio de envio por e-mail ou outro sistema, deverá ser aberta concorrência para contratação de ferramenta DLP própria para este tipo de aplicação em específico.

A aplicabilidade e o tipo de ferramenta DLP deverão ser definidos pelas áreas de Segurança da Informação ou mesmo pelo Comitê de Riscos e *Compliance*.

4.15. Teste de Intrusão e Scan de Vulnerabilidades

No mínimo 1 (uma) vez por ano são realizados testes de intrusão e *scan* de vulnerabilidades para a prevenção de vazamento de informações, checagem de proteção contra *software*s maliciosos e detecção de aderência de *patches* de *software*.

O escopo é interno e externo, abrangendo sistemas internos de Tecnologia e de Negócios. Farão parte dos testes os *firewalls* de borda de Internet, testando conexões e IPs externos da rede.

Apenas empresas especializadas serão contratadas para a execução do trabalho.

4.16. Contrato com Fornecedores

Todos os contratos fechados com fornecedores deverão ser aderentes às leis, normas e procedimentos definidos por órgãos reguladores e autorreguladores que regem as empresas do Grupo BR Partners.

Havendo a intenção de contratação de serviços em nuvem, além de serem homologados pelas áreas envolvidas quanto aos requisitos técnicos e funcionais, o órgão regulador pertinente deverá ser comunicado acerca da intenção da sua contratação com antecedência mínima de 60 (sessenta) dias.

4.17. Disseminação da Cultura

Esforços relacionados à Segurança Cibernética e da Informação não alcançam a eficácia pretendida sem a devida abordagem de Pessoas, ou seja, os colaboradores da corporação. Para este fim, são estabelecidos mecanismos para disseminação da cultura da segurança cibernética na instituição, a saber:

- Criação e gestão de Programa de Cônscio e Capacitação em Segurança Cibernética que preveja a adoção de canais de comunicação e disseminação da cultura da segurança cibernética;

- Criação e disseminação de palestras e treinamentos, circulares internas, intranet com recursos de texto, áudio e vídeo e outros, abordando e explanando sobre o tema. Estas ações são extensíveis a parceiros de negócios, fornecedores e prestadores de serviços do Grupo BR Partners;
- Temas como Segurança Cibernética, da Informação, Engenharia Social, Malwares, Comportamento Seguro, Proteção de Dados Impressos e correlatos são abordados periodicamente em palestras e treinamentos internos, bem como nos demais canais de comunicação internos;
- Aplicação de cursos, treinamentos ou outros mecanismos para checagem da absorção do conhecimento são realizadas de maneira constante. Seus resultados são tabulados e geridos pelo departamento de Recursos Humanos do Grupo BR Partners. Reciclagens são providenciadas sempre que necessário; e
- Assinatura de *N.D.A.* (no ato da contratação ou antes da assinatura de um contrato) que promova a Confidencialidade da informação, são devidamente providenciados. Da mesma forma, assinatura de aceites da Política de Segurança Cibernética e da Informação, do Código de Conduta e demais documentos correlatos são devidamente providenciados e armazenados.

4.18. Implementação de Programas de Capacitação

Parte fundamental na gestão de riscos cibernéticos, os colaboradores são inseridos e reciclados quanto aos seus conhecimentos sobre o tema. Um Programa de Cônscio e Capacitação em Segurança Cibernética foi construído e é ministrado de maneira recorrente, determinando necessidade de:

- Treinamento constante sobre o tema para todos os colaboradores do Grupo BR Partners, em todos os níveis hierárquicos, especialmente àqueles que são recém-admitidos;
- Avaliação de absorção do conhecimento é ministrado a todo colaborador que participa deste programa, ministrado e gerido pelo departamento de Recursos Humanos (ou por indicação deste), promovendo reciclagens sempre que necessário;
- Execução de testes específicos e pontuais, que visem identificar falhas entre conhecimento e procedimentos operacionais praticados pelas áreas de negócio, que possam afetar as práticas de Segurança Cibernética e da Informação. Seus resultados são tabulados e compartilhados periodicamente com os gestores diretos e diretoria responsável;
- Todo colaborador deve participar, no mínimo, de dois treinamentos anuais, com temas relacionados Segurança Cibernética e/ou da Informação e seu nível de absorção de conhecimento deve estar acima da nota de corte vigente.

4.19. Prestação de Informações sobre Produtos e Serviços

A área de *Compliance* do Grupo BR Partners é responsável pela gestão da Política de Relacionamento com Clientes, estabelecendo os princípios e diretrizes que devem ser seguidos pelos colaboradores, parceiros de negócio e prestadores de serviços contratados, no que se refere ao relacionamento com o cliente durante todas as fases de contratação e pós-contratação dos produtos e serviços ofertados pelo Grupo BR Partners.

Tal Política de Relacionamento com Clientes zela pelos mais rígidos padrões de ética, responsabilidade, transparência e integridade corporativa, para que sua atuação no mercado se dê em observância às leis, regulamentos e boas práticas de governança e atendimento ao cliente.

4.20. Iniciativas para Compartilhamento de Informações

Relatório executivo com tabulação dos principais incidentes cibernéticos ocorridos e tratados é produzido, validado, aprovado e então e compartilhado com outras instituições financeiras, promovendo a troca de conhecimento e evolução das ações relacionadas à Segurança Cibernética e da Informação em instituições deste segmento, nacionais ou internacionais.

Neste relatório são registrados os incidentes, sua causa-raiz, as ações compensatórias adotadas, a revisão dos controles de segurança envolvidos e os resultados alcançados após compensação.

Estes relatórios são compartilhados em fóruns apropriados e destinados a esta finalidade somente pelos representantes legais, incumbidos desta tarefa pela alta direção do Grupo BR Partners.

4.21. Plano de Resposta de Incidente de Segurança da Informação

O procedimento de resposta a incidentes de segurança da informação é composto de etapas necessárias para prover uma abordagem bem definida e organizada para manusear os incidentes de segurança da informação de forma eficiente. Sempre que um evento é reportado como incidente de segurança da informação, o BR Partners deve acionar o procedimento do Manual de Plano de Resposta a Incidentes de Segurança da Informação para executar atividades apropriadas**.**

5. REVISÃO

Este Manual da Política deverá ser revisado, no mínimo, anualmente.

6. DOCUMENTOS RELACIONADOS

Política de Segurança da Informação

Manual da Politica de Segurança da Informação

7. LEGISLAÇÃO E REGULAÇÃO

Resolução nº 4.658/18 do Conselho Monetário Nacional (CMN)