BR CAPITAL
distribuidora de títulos e valores mobiliários

Política de Segurança Cibernética e da Informação

Av. das Nações Unidas 11857 – 111. – São Paulo - SP – Brasil – 04578-000
fone: 55-11-5508-3500; fax: 55-11-5506-4033; brcapital@brcapitaldtvm.com.br
OUVIDORIA: fone: 0800-777-3505; ouvidoria@brcapitaldtvm.com.br

Assunto: Política de Segurança Cibernética e da Informação

1. Objetivo

A Política de Segurança Cibernética e da Informação é uma declaração formal da **BR|CAPITAL** acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus Funcionários / Colaboradores.
A Política de Segurança Cibernética e da Informação se baseia em padrões de mercado visando também tratar de modo mais abrangente a governança e o gerenciamento de riscos da informação dentro **BR|CAPITAL**.

2. Legislação Vigente

Esta Política tem como objetivo atender a resolução nº 4.658 do Banco Central do Brasil, NBR ISSO 27002, Lei 9.609/98 – Software, Guia de Cibe segurança - ANBIMA entre outras.

3. Abrangência

Esta Política aplica-se a todos os Administradores, Funcionários, Colaboradores e Prestadores de Serviços.

4. Princípios de Segurança da Informação

A Política de Segurança Cibernética e da Informação visa garantir a proteção das informações institucionais de diversos tipos de ameaça, de forma consistente visando a minimização aos danos e maximização do retorno dos investimentos e das oportunidades de negócio.
A segurança da informação é aqui caracterizada pela preservação da:

- Confidencialidade, que é a garantia de que a informação é acessível somente as pessoas com acesso autorizado;
- Integridade, que é a salvaguarda da exatidão e o conteúdo da informação e dos métodos de processamento;
- Disponibilidade, a Política de Segurança Cibernética e da Informação deve ser divulgada a todos os Funcionários / Colaboradores e disponibilizadas de maneira que seu conteúdo possa ser consultado a qualquer momento; e
- Acesso controlado, significa que os Funcionários / Colaboradores terão controle sobre as informações a serem identificadas e processadas de forma a mitigar ameaças à segurança da informação ou possíveis quebras da confidencialidade delas.

Para assegurar esses princípios, as atividades de segurança da informação devem ser adequadamente gerenciadas e protegidas contra roubos, fraudes, espionagem, perda não intencional, acidentes e outras ameaças.
É fundamental para a proteção e salvaguarda das informações que os Funcionários / Colaboradores adotem a ação de "comportamento seguro e consistente" com o objetivo de proteção das informações, devendo assumir atitudes proativas e engajadas.

Campanhas contínuas de conscientização de Segurança da Informação serão utilizadas para monitoração e controle desses princípios.
A Política de Segurança Cibernética e da Informação da **BR|CAPITAL** deve ser revisada e aprovada anualmente pela Diretoria Executiva.

5. Atribuições e Responsabilidades na Gestão de Segurança da Informação

Cabe a todos os Funcionários, Colaboradores, Prestadores de Serviços e outros cumprir fielmente a Política de Segurança Cibernética e da Informação; buscando orientação no gestor imediato em caso de dúvidas relacionadas à segurança da informação; proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados; assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela **BR|CAPITAL**; cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual; e comunicar imediatamente a empresa quando do descumprimento ou violação desta Política.
Casos de violação de segurança da informação devem ser comunicados através de e-mail ao seu Superior e/ou a área de Compliance.
A violação dos princípios, normas e/ou diretrizes ou a não aderência a esta Política são consideradas faltas graves ou violações, podendo ser aplicadas as seguintes penalidades ou sanções:

- aplicação de sanções trabalhistas previstas em legislação vigente, incluindo dispensa por justa causa;
- processo civil ou criminal;
- ressarcimento dos prejuízos causados à Instituição; e/ou,
- aplicação de outras ações disciplinares constantes na legislação brasileira vigente.

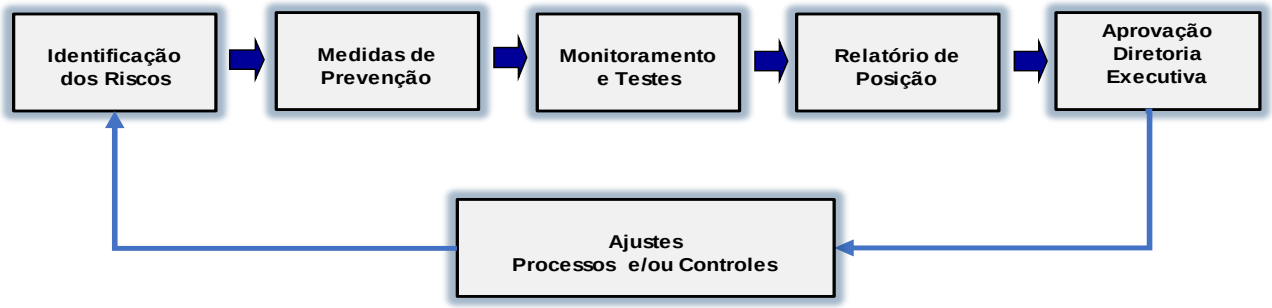
Área de Tecnologia e Compliance
Cabe as duas áreas propor ajustes, melhorias, aprimoramentos e modificações desta Política; convocar, coordenar, lavrar atas e prover apoio às reuniões que discutam a respeito desta; prover todas as informações de gestão de segurança cibernética e da informação.

Informações Complementares

- ✓ A empresa Alest Consultoria é responsável pelos serviços de gerenciamento de backup de segurança e controle dos arquivos em servidores instalados no Brasil.

6. Implantação e Controles

Plano de Segurança Cibernética



I. Identificação dos Riscos

O processo de avaliação de riscos de segurança cibernética tem como base a *Matriz de Riscos, documento que faz parte e completa esta Política*.

Essa Matriz tem por finalidade identificar os ativos relevantes da instituição (equipamentos, sistemas, dados, backup, meios de comunicação e outros); regras para a classificação das informações geradas pela instituição; riscos / possíveis impactos (financeiros, operacionais, reputacionais entre outros) e ações de mitigação desses possíveis riscos.

II. Medidas de Prevenção

Para mitigar muitos dos riscos de segurança cibernética os principais controles estão relacionados ao acesso adequando aos ativos da **BR CAPITAL**.

A implementação desses controles passa pelos Procedimentos de Segurança Operacional, conforme descritos no Item 5.

Anualmente ou quando houver demanda específica, os Funcionários / Colaboradores devem passar por treinamento sobre os procedimentos de Segurança Cibernética e da Informação; como também, no Plano de Continuidade de Negócio – PCN.

III. Monitoramento e Testes

Os mecanismos de monitoramento das ações de proteção devem manter:

- Inventários atualizados de hardware e software;
- Atualizados os sistemas operacionais e softwares de aplicação instalados;
- Monitoramento diariamente das rotinas de backup, executando testes regulares de restauração dos dados;
- Testes de invasão externa;
- Análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura.
- Análises dos logs e as trilhas de auditoria criados, de forma a permitir a rápida identificação de ataques, sejam internos, sejam externos.

IV. Relatório de Posição

A **BR|CAPITAL** deve elaborar o Relatório de Posição (Relatório Anual - Segurança Cibernética) sobre a implementação do Plano de Segurança Cibernética e de respostas à incidentes relativos ao ano civil, contendo:

- Validação das rotinas e procedimentos adotados quanto a segurança cibernética;
- Análise das causas e dos impactos ocorridos;
- Resumo dos resultados obtidos utilizados na prevenção e respostas a incidentes;
- Resultado dos testes de continuidade dos negócios.

Arquivar o Relatório Anual – Segurança Cibernética pelo período de 5 anos da data de elaboração.

V. Aprovação da Diretoria Executiva

O Relatório Anual – Segurança Cibernética deve ser apresentado à Diretoria Executiva, até 31 de março do ano seguinte ao da data base, e estar disponível na sede da instituição para consulta pelos órgãos reguladores.

VI. Ajustes nos Processos e/ou Controles

O Plano de Segurança Cibernética deve ser revisado periodicamente, conforme definido nesta Política, mantendo sempre atualizadas suas avaliações de risco, implementações de proteção, planos de resposta a incidentes e monitoramento dos ambientes.

A **BR|CAPITAL** deve promover e disseminar a cultura de segurança através de treinamentos e de canais de divulgação que sejam eficientes para difundir o programa de segurança cibernética; assim como, conscientizar seus Funcionários / Colaboradores sobre os riscos e as práticas do assunto em questão.

7. Atribuições e Responsabilidades - Tecnologia da Informação

Cuidar do planejamento, organização e execução das atividades de Tecnologia – Segurança Cibernética, fornecendo soluções alinhadas às metas e aos objetivos da instituição, apoiando e otimizando produtos e serviços a clientes, o processo operacional, bem como, o fornecimento de informações para tomada de decisões.

Diretor responsável pela Segurança Cibernética

O Diretor responsável pela Segurança Cibernética passa também a desempenhar, em conjunto com as áreas de Tecnologia e de Compliance as atribuições estabelecidas na Resolução nº 4.658 do BACEN; mas de forma que não haja conflito de interesses em relação às funções, cabendo a este:

- Propor o desenvolvimento de ações para adequar a estrutura funcional aos princípios e às diretrizes desta Política;

- Definir em conjunto com os demais envolvidos as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes; e
- Coordenar em conjunto com os demais envolvidos: o registro, os controles dos efeitos de incidentes relevantes e de respostas a incidentes.

Responsável pela área de Tecnologia

- Planejar, implantar e gerenciar o uso dos recursos de informática da instituição, em linha com os planos estratégicos de negócios e operacionais, adotando tecnologias e métodos que melhor se adequem a este objetivo e garantam o cumprimento dos requisitos legais, da segurança cibernética e dos controles estabelecidos pelas normas internas e externas, dentre outros.
- Garantir o processamento das transações, visando a qualidade, integridade e rapidez das informações produzidas.
- Definir os padrões de hardware e software e recomendar a aquisição de recursos de informática.
- Administrar os recursos de informática e prover as tecnologias e meios necessários para que eles sejam devidamente utilizados.
- Assegurar a capacitação ao nível adequado do pessoal de informática sobre o entendimento dos negócios da instituição.
- Analisar viabilidade técnica/ financeira de utilização de recursos de informática (software, sistemas, aplicativos, hardware e outros) próprios ou de terceiros.
- Elaborar guias de desenvolvimento e gerenciamento de projetos de informática e coordenar o treinamento do pessoal envolvido nos mesmos.
- Fornecer meios para captação de informações gerenciais.
- Garantir a adequada proteção e integridade dos dados, tais como armazenamento, transmissão, backup, antivírus, gerenciamento de “senhas”, segregação de funções entre outros.
- Prestar suporte à Auditoria referente as trilhas de auditoria que possam ser verificadas, a fim de garantir o nível de controles internos da organização.

Responsável pela área de Compliance

A área de Compliance deve:

- Desenvolver e acompanhar a implantação dos controles internos, bem como promover testes periódicos incentivando a realização de provas e verificação de dados.
- Realizar em conjunto com a área de Tecnologia a avaliação quanto ao desempenho dos procedimentos de controles executados, exposição dos riscos e situação dos planos de ação desenvolvidos.
- Avaliar periodicamente os canais de comunicação, verificando se as informações estão disponíveis a todos os Funcionários / Colaboradores, de acordo com o seu nível de atuação, de forma confiável e compreensível, desde que relevantes para suas tarefas e responsabilidades.
- Participar dos treinamentos e testes de segurança cibernética e da informação.

Demais Gerências e Diretoria(s)

As demais Gerências e Diretoria(s) deverão:

- Garantir uma ativa participação dos Usuários nos processos de planejamento, desenvolvimento e implantação dos projetos de TI; como também, nos de segurança cibernética e da informação.
- Garantir que o uso dos recursos de informática contribua para a melhora da rentabilidade, controles e otimizações de processos da organização.
- Garantir que estejam adequadamente definidas as solicitações para a área de Tecnologia.
- Aprovar/ homologar dentro dos prazos acordados no plano de trabalho de cada um dos projetos que impactam a área, os produtos a serem entregues em cada uma de suas fases, assegurando que revisões sejam efetuadas por pessoas apropriadas e de responsabilidade comprovada.
- Criar as condições necessárias, em termos de recursos humanos e materiais, para o uso adequado dos recursos de informática, assegurar que eles sejam aceitos e bem utilizados pelos Usuários.
- É de responsabilidade da área em questão que estiver interessada em inscrever algum Funcionário / Colaborador em cursos externos de informática, realizar a solicitação para a análise e/ ou indicação da área de Tecnologia.
- Assegurar que estão sendo tomadas medidas de proteção das informações que circulam pela sua(s) área(s) de responsabilidade, garantir que os acessos estejam adequados e identificar riscos e exposições.

Usuários

Os Usuários deverão:

- Participar ativamente nos processos de planejamento, desenvolvimento e implantação de novas ferramentas tecnológicas para racionalização e otimização das rotinas operacionais e de segurança da informação.
- Garantir que os dados de sua propriedade sejam protegidos contra acessos não autorizados.
- Respeitar as normas internas e externas de segurança, proteção à informação e outros.
- Somente utilizar software, sistemas aplicativos ou hardware registrados e homologados pela área de Tecnologia.
- Manter todos os dados de uso nos diretórios da rede, para que não haja perdas de informações.

8. Plano de Ação e de Resposta a Incidentes

Caberá a área de Tecnologia definir os recursos a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes da Política de Segurança Cibernética e da Informação quanto a:

- Definição de processos, testes e trilhas de auditoria;
- Definição de métricas e indicadores adequados; e
- Identificação e a correção de eventuais deficiências.

Com base nessas premissas, o Plano deve detalhar:

1. A ferramenta de controle para registro de ocorrência de incidente seja para a correção de alguma funcionalidade, correção de algum erro de tratamento e/ou correções em conteúdo de dados;
2. Pontos de controle: realização periódica de auditoria de melhores práticas, segurança e pontos falho.
3. Correções e melhorias: atualização / manutenção da(s) ferramenta(s) com novas funcionalidades, controles e recursos tecnológicos.
4. Registro, divulgação e orientação do posicionamento quanto à Segurança Cibernética a todos os Funcionários / Colaboradores da **BR|CAPITAL**; como também, aos órgãos reguladores.

A Implementação do Plano de Segurança Cibernética está sob a coordenação do Diretor responsável pelo assunto mais as áreas de Tecnologia e Compliance; e contempla a:

- Contratação da empresa de prestação de serviços a *Alest Consultoria*, visando o fornecimento de alocação de infraestrutura na "Nuvem", servidor de dados, servidor de base de dados, rotinas de backup, recuperação de backup, incidentes da plataforma, checagem de segurança e pontos de melhoria, atualizações e melhorias constantes.
- Certificação do BACEN quanto a empresa contratada. Prazo em conformidade com o da contratação da *Alest Consultoria*, Isos e certificação da Google.
- Implantação dos processos e procedimentos da Plataforma de Gestão com os procedimentos de rotinas de backup e recuperação de informações; como também, rotinas para o tratamento de incidências e outros eventos.
- Revisão dos processos e controles quanto aos "backups" e "arquivo de documentos / informações".
- Treinamento e divulgação dos Funcionários / Colaboradores da instituição.
- Teste de segurança dos procedimentos implantados.
- Teste de verificação anual de possíveis ocorrências de incidentes.
- Apresentação e aprovação das atividades relacionadas à Segurança Cibernética: Ações e Respostas a Incidentes, para a Diretoria Executiva.
- Relatório Anual – Segurança Cibernética.

9. Procedimentos de Segurança Operacional

Entende-se por "recursos de informática" os recursos utilizados para o tratamento de informações, incluindo computadores, equipamentos, sistemas, softwares, rede comunicações, base de dados, acessos, dados armazenados em meios magnéticos e outros.

Como também a implantação da “Plataforma de Gestão” através de ferramentas para a redução de vulnerabilidade local e nas nuvens, que tem por finalidade processar as rotinas de backup e recuperação de informações; assim como os registro e tratamento das incidências.

Corporativo

A rede de computadores deverá ser administrada de forma que os recursos sejam operados e gerenciados de forma segura.

O ambiente de rede deverá ser garantido contra-ataques externos (*Firewall*).

Arquivos de origem desconhecida ou não originados dentro da empresa ou não relacionados com os negócios (provenientes de unidades removíveis), não devem ser abertos ou copiados em hipótese alguma.

Compartilhamento de senhas entre Usuários não são permitidos em hipótese alguma.

Todo Usuário deverá, obrigatoriamente, autenticar-se na rede de computadores através de “login” e “senha” próprios com acessos compatíveis à sua função.

O “login” de rede deverá ser bloqueado após 3 (três) tentativas sucessivas de acesso com senha incorreta.

A senha deverá ser substituída a cada 90 dias, possuir no mínimo 6 caracteres e, ainda, deverá ser diferente das últimas 4 senhas utilizadas.

Á área de Tecnologia deve desenvolver o Plano de Continuidade de Negócios – PCN junto com os demais envolvidos; visando garantir a recuperação dos processos críticos do negócio durante eventual indisponibilidade do ambiente computacional.

A segregação de funções entre Administradores e Usuários de sistemas / aplicativos deverão ser obedecida.

Os sistemas e serviços oferecidos pela **BR|CAPITAL** os que são, necessariamente, acessados por internet, devem ser hospedados em Datacenter independente da rede interna de computadores.

Processamento e Armazenamento de Dados

Conforme a Resolução 4.658/2018 do BACEN, a **BR|CAPITAL** contratou os serviços de processamento e armazenamento de dados e de computação em nuvem, assegurando assim, um procedimento efetivo para a aderência às regras previstas na regulamentação em vigor.

As cópias de segurança de sistemas, ferramentas e/ou aplicativos são feitas de forma centralizada no ambiente do servidor corporativo, sob a responsabilidade da área de Tecnologia. As cópias de segurança também são enviadas para a unidade de contingência.

São realizados 3 (três) tipos de backup:

- Backup diário, na qual devem ser armazenados todos os dias da semana, que armazena as 5 últimas modificações realizadas em todos os arquivos;

Os backups são efetuados em duas vias, sendo uma delas guardada em empresa externa especializada de “storage na nuvem” e outra na unidade de contingência.

Backups dos arquivos das unidades de trabalho, diretórios e outros são efetuados:

- Storage em rede: visando fornecer o armazenamento físico de arquivos distribuídos na rede de forma que se obtenha maior capacidade e desempenho dos dados.
- Storage na nuvem: visando os serviços de gerenciamento de backup de segurança e controle dos arquivos em servidores instalados no Brasil. Desta forma é possível não apenas armazenar, mas também transferir os arquivos do servidor para o site de contingência e possibilita o monitoramento constante dos dados armazenados.

Contingência Operacional

Caberá a área de Compliance estabelecer a Política e diretrizes que permitam o detalhamento dos programas de proteção / contingências e o Plano de Continuidade de Negócios - PCN relativos aos sistemas e ambientes de tecnologia da informação.

A área de Compliance deverá:

- Assegurar o cumprimento, no dia a dia, das diretrizes estabelecidas;
- Elaborar e implementar programas e plano de contingência que assegurem a proteção e integridade física dos dados, dos ambientes e equipamentos de processamento e que permitam, em situações emergências, reação imediata e rápida recuperação das informações, sem prejuízo das rotinas operacionais essenciais à condução dos negócios da organização;
- Revisar, periodicamente, suas instalações, a fim de assegurar o funcionamento dos sistemas de segurança do local de processamento de dados, tais como sistema de acesso, controles de temperatura e umidade ambiental, extintores entre outros;
- Divulgar os programas de proteção e planos de contingência, de forma a assegurar que todos os Funcionários / Colaboradores da **BR|CAPITAL** saibam quais são suas funções e responsabilidades em caso de contingência ou desastre;
- Revisar o “Plano de Continuidade de Negócios - PCN”, anualmente ou sempre que necessário.

Procedimentos de Segurança e Acesso

Acesso a Arquivos e Diretórios

Os Usuários não devem ter acesso direto às bases de dados, e sim apenas através dos respectivos sistemas aplicativos.

Os Usuários não devem ter direitos de alteração e/ou exclusão de programas.

Os Usuários só devem ter direito de salvar arquivos nos seus volumes e pastas específicos.

Os Usuários devem possuir permissões de acesso mínimas, suficientes para utilizar os recursos requeridos pela sua função.

Acesso a Conexão Externa

Deve ser bloqueado, salvo as explicitamente autorizadas pelo Diretor responsável por tratar-se de equipamento crítico, o firewall deve possuir sistema de redundância ativa.

É expressamente proibido o acesso a páginas da Internet de conteúdo relacionado a Crimes, Drogas/Álcool, Erotismo, Sexo Explícito, Hackers, Jogos Eletrônicos ou de Azar, Música ou Rádio, Racismo e Violência**.**

O acesso dos Usuários via Internet é filtrado por um analisador de conteúdo, que bloqueia o acesso a sites considerados não autorizados de acordo com o seu perfil de acesso, através de listas com atualização diária. Porém, o fato de ser possível o acesso a um determinado site não significa que esse acesso seja permitido.
É vedado aos Usuários o acesso a sites com conteúdo considerado ilegal, pornográfico ou impróprio. Os arquivos baixados da Internet são filtrados por um analisador de conteúdo que bloqueia o acesso a arquivos sob suspeita de vírus.
As mensagens eletrônicas enviadas e recebidas pelos Usuários são filtradas por um analisador de conteúdo, que remove arquivos anexos não permitidos para cada perfil de acesso ou sob suspeita de vírus.
Responsabilidades
É responsabilidade da área de Tecnologia a definição das políticas de segurança e acesso aos recursos de TI disponíveis.
Cabe à área de Tecnologia a implementação no firewall das políticas de segurança e acesso a recursos aprovados pela Gerência / Diretoria.

Autenticação dos Usuários
Descrição
Usuários são autenticados na rede através de um par “login” /” senha” para acesso aos recursos disponibilizados internamente (impressoras, compartilhamentos) e externamente (Internet, RTM e redes corporativas conectadas).
Cada sistema aplicativo utilizado possui um sistema de autenticação de Usuário independentemente da autenticação da rede, para acesso às suas funções.
Procedimentos de Segurança e Acesso
A senha de autenticação na rede deve ser substituída a cada 90 dias, deve ter no mínimo 6 caracteres (letras e números) e deve ser diferente das 4 últimas senhas utilizadas.
Os Usuários devem obrigatoriamente se autenticar perante a rede e perante cada sistema aplicativo utilizado, não sendo permitido o fornecimento de senhas para outros Usuários ou a utilização de senhas de outros Usuários para acesso à rede ou aos sistemas.
Solicitações de cadastramento de novo usuário na rede e nos sistemas aplicativos devem ser solicitadas pelos gerentes das respectivas áreas.
Demissões de funcionários devem ser imediatamente comunicadas ao Administrador da Rede, para descadastramento na rede e nos sistemas.
Responsabilidades
É responsabilidade dos gerentes notificar a área de Tecnologia para a inclusão de Usuário na rede em caso de contratação de novo Funcionário / Colaborador ou para a exclusão em caso de demissão ou desligamento.
É responsabilidade de cada Usuário manter em sigilo a(s) sua(s) senha(s) de acesso à rede e aos sistemas aplicativos utilizados.
É responsabilidade da área de Tecnologia a alteração das senhas dos Usuários na rede quando necessário.

Circuitos de Comunicação

Descrição

A instituição possui alguns circuitos de comunicação contratados com as operadoras de telecomunicações de forma a permitir o acesso à recursos disponibilizados nas redes.

Procedimentos de Segurança e Acesso

Todos os circuitos de comunicação críticos devem possuir um segundo circuito alternativo, em meio ou operadora diferente, como contingência. Mesmo os circuitos não críticos devem possuir esquema de contingência.

Eventuais circuitos de comunicação estabelecidos através de redes públicas devem obrigatoriamente ser implementados através de túneis criptografados com criptografia forte e chaves trocadas periodicamente.

Todos os circuitos externos de comunicação devem estar conectados à rede da instituição através do firewall.

Responsabilidades

É responsabilidade das operadoras de telecomunicações contratadas a manutenção do nível de serviço acordado em contrato.

A área de Tecnologia é responsável pela contratação ou cancelamento de circuitos de comunicação conforme a necessidade.

É responsabilidade da área de Tecnologia dar suporte à contratação ou cancelamento de circuitos de comunicação, configurar o firewall de forma a permitir o acesso aos recursos externos de forma segura e acionar a respectiva operadora de telecomunicações em caso de problemas em um circuito de comunicação e acionar o plano de contingência.

Rede Local

Descrição

Os servidores e as conexões de outros equipamentos de rede estão conectados de forma a otimizar o tráfego e a performance geral da rede. A conexão uplink foi implementada através do módulo que permite a comunicação em alta velocidade. As impressoras estão desvinculadas das estações de trabalho e conectadas diretamente à rede.

Procedimentos de Segurança e Acesso

Todos os switches críticos devem possuir equipamento de contingência. Todos os pontos do cabeamento estruturado ociosos devem estar obrigatoriamente desconectados da rede local. Apenas máquinas de propriedade da empresa ou explicitamente autorizadas pela área de Tecnologia podem ser conectadas à rede local.

Responsabilidades

É responsabilidade da área de Tecnologia / Administrador da Rede conectar ou desconectar pontos do cabeamento físico aos hubs / switches.

Estações de Trabalho

Descrição

A **BR|CAPITAL** disponibiliza ao seu corpo de Funcionários / Colaboradores estações de trabalho para a execução das suas funções, quando necessário.

Procedimentos de Segurança e Acesso

É expressamente proibido aos Usuários:

- Instalação de softwares adicionais, sem homologação pela área de Tecnologia.
- Manipulação de componentes das estações de trabalho ou a abertura do seu gabinete.
- Evasão de quaisquer arquivos ou informações, por qualquer meio, sem a devida autorização da área competente.

Todas as informações processadas e armazenadas nas estações de trabalho da **BR|CAPITAL** sejam estas em forma de bancos de dados, documentos, planilhas ou qualquer outro tipo de arquivo são de propriedade exclusiva dela, podendo esta dispor desses recursos da forma que melhor lhe aprouver.

Responsabilidades

É responsabilidade da área de Tecnologia a manutenção, instalação e configuração do software necessário nas estações de trabalho.

É responsabilidade do Usuário zelar pelo equipamento a ele confiado e notificar à área de Tecnologia quaisquer problemas por ele verificados.

Infraestrutura Básica de Serviços

Energia elétrica:

- Servidor: alimentação por nobreak com autonomia de 2 horas.
- Estações de trabalho: alimentação por nobreak com autonomia de 30 minutos.
- O Edifício aonde a **BR|CAPITAL** está sediada possui gerador que é ativado após o período de 10 segundos, com capacidade de demanda de até 8 horas.

Telefonia:

- Central Embratel E1(R2dDigital) com 14 linhas digitais (VOIP) com faixa de numeração de 50 DDR;

Internet:

- Banda Larga – NET com 60GB.
- Banda Larga – Vivo Fibra ÓTICA 30GB.
- Banda Larga – Embratel Fibra Ótica 1GB.

10. Responsabilidade

A Diretoria Executiva da **BR|CAPITAL** se compromete com a melhoria contínua dos procedimentos e controles relacionados nesta Política, os quais devem ser objetos de pautas recorrentes.

Esta Política deve ser revisada e/ou atualizada anualmente, de forma a evidenciar a sua apreciação, discussão e reformulação através de Ata de Reunião.

Quaisquer indícios de irregularidades no cumprimento das determinações desta Política serão alvo de investigação interna e devem ser comunicadas imediatamente através de e-mail ao seu Superior e/ ou a área de Compliance.

* * *

Diretor Responsável: Carlos Orlandelli Lopes.

Aprovação: Diretoria Executiva.

Canal de Comunicação*: E-mail:* compliance@brcapital.com.br

* * *

ANEXO I

Termo de Responsabilidade de Segurança da Informação

Atesto ter recebido, lido e compreendido os princípios e diretrizes da Política de Segurança Cibernética e da Informação **BR-CAPITAL DISTRIBUIDORA DE TÍTULOS E VALORES MOBILIÁRIOS S.A.** - **BR|CAPITAL** comprometendo-me a observá-la integralmente e comunicar ao meu Superior e/ou a área de Compliance sobre qualquer inconformidade que venha a ser de meu conhecimento.
Declaro ter pleno conhecimento que o descumprimento da Política e deste Termo pode implicar em demissão, inclusive por justa causa, sem prejuízo de apuração dos danos que tal descumprimento possa causar a Instituição.

Data: _____/_____/_____

Assinatura:_____
Nome:
RG:
Cargo: