



BRASIL
PLURAL

Manual de Segurança a Informação

Setembro de 2016

Elaboração: Compliance

Revisão: Comitê de Segurança da Informação

Próxima revisão: Setembro de 2017.

Aprovação: Diretoria de Meios

Classificação do Documento: INTERNO (Acesso e manuseio restritos aos colaboradores do Brasil Plural. Uso externo somente com validação de Compliance).

ÍNDICE

1.	Introdução	4
2.	Objetivo e Abrangência	4
3.	Estrutura Organizacional em Segurança da Informação	6
3.1.	Papéis e Responsabilidades	7
	Comitê de Segurança da Informação.....	7
	Área de Segurança	7
	Compliance	8
	Jurídico	8
	Área de Gente	9
	Risco	9
	Processos	9
	Administrativo	9
	Tecnologia da Informação	10
	Cadastro	11
	Auditoria Interna.....	12
	Áreas Comerciais e de Relacionamento com Clientes.....	12
	Membros do Comitê Executivo e Diretoria	12
	Gestores das Áreas	12
	Demais Colaboradores.....	13
4.	Classificação das Informações	13
4.1.	Relevância e Integridade	13
4.2.	Disponibilidade	14
4.3.	Retenção	14
5.	Tratamento e proteção dos ativos de informação	15
5.1.	Guarda de Informações	15
5.2.	Acesso Físico e Lógico	15
	Acesso Lógico	16
	Acesso Físico	16



Política de Senhas	16
5.3. Mídias e Recursos Portáteis.....	17
5.4. E-mail e Telefonia	18
5.5. Uso da Internet	18
5.6. Utilização de Software	19
5.7. Descarte de Informações	20
5.8. Comunicação Verbal	20
5.9. Incidentes de Segurança	20
6. Resumo das principais vedações	20
7. Treinamento	21
8. Considerações finais	21

1. Introdução

Este Manual de Segurança das Informações (o “Manual”) foi desenvolvido com o intuito de estabelecer as diretrizes e melhores práticas necessárias para a proteção de nossas informações, bem como informações de terceiros armazenadas em nossa estrutura, principalmente as de clientes.

Trata-se de um documento que contempla um conjunto de princípios, práticas e cuidados mínimos necessários que norteia a gestão de segurança de nossas informações corporativas.

Este documento é aplicável a todos os estagiários, funcionários, sócios, fornecedores, prestadores de serviços e parceiros comerciais do Grupo Brasil Plural (“colaboradores”) e será regularmente atualizado e divulgado pela área de Compliance, responsável também pelo monitoramento e estabelecimento de procedimentos e mecanismos de controles internos que visem à observância das disposições aqui contidas.

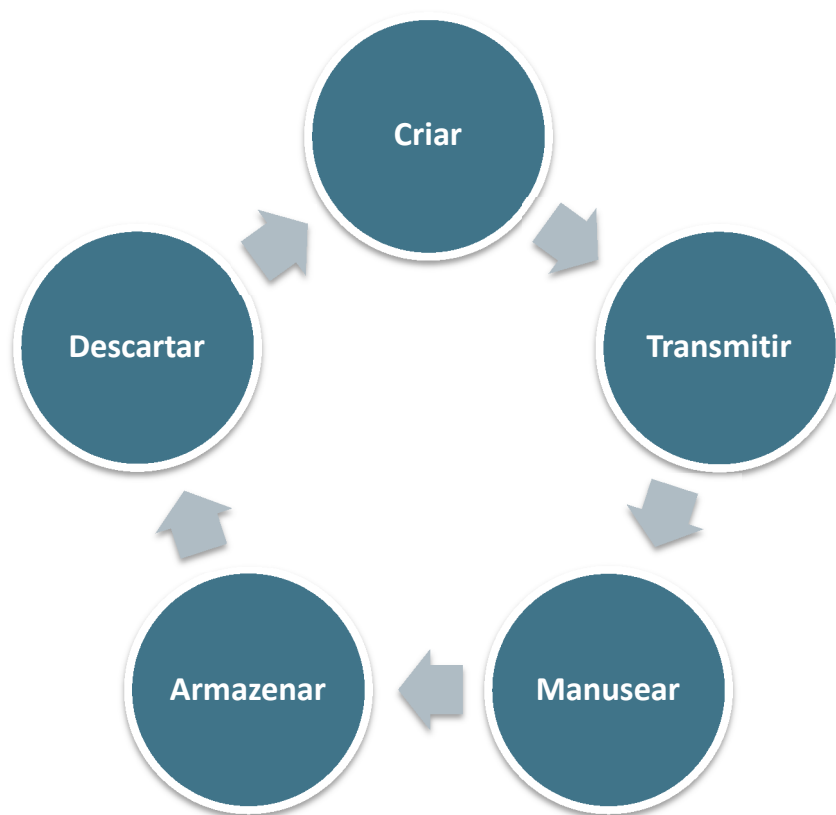
Em linha com as expectativas do Comitê Executivo do Grupo Brasil Plural, é responsabilidade de todos a implementação e o cumprimento das regulamentações aplicáveis sobre o tema e de todo o conteúdo deste Manual.

Como colaborador do Grupo Brasil Plural, para assegurar a eficácia dos procedimentos e controles transcritos ao longo deste documento, você deve tomar conhecimento sobre suas funções e responsabilidades específicas sobre o assunto, bem como zelar pelo cumprimento das mesmas.

2. Objetivo e Abrangência

Este Manual foi desenvolvido com o objetivo de definir regras, responsabilidades e estratégias essenciais relacionadas aos procedimentos e mecanismos de controles internos visando minimizar os impactos associados à ação de ameaças e riscos em todo o “ciclo de vida de cada informação”.

A abrangência das regras e controles aqui dispostos refere-se ao ciclo de vida físico e lógico da informação, conforme ilustrado e detalhado abaixo:



Fase / Meio	Meio Físico	Meio Lógico
Criar	<i>Documentos gerados e disponibilizados pelo Grupo Brasil Plural.</i>	<i>Bases de dados e informações geradas e disponibilizadas pelo Grupo Brasil Plural.</i>
Transmitir	<i>Documentos (inclusive mídias móveis) que circulam internamente ou aqueles recebidos e enviados (externamente).</i>	<i>Transmissão ou recebimento de arquivos e informações eletronicamente (ou por telefonia).</i>
Manusear	<i>Uso e acesso a informações e dados físicos (inclusive mídias móveis).</i>	<i>Uso e acesso a informações e dados lógicos (inclusive mídias móveis).</i>
Armazenar	<i>Formas de acesso e organização do armazenamento de documentos e mídias em locais físicos internos ou externos.</i>	<i>Arquivos de dados de documentos e informações eletrônicas.</i>
Descartar	<i>Fragmentação de documentos físicos e mídias.</i>	<i>Exclusão de dados e informações lógicas.</i>

3. Estrutura Organizacional em Segurança da Informação

Acreditamos que a melhor prática para se gerir a segurança das informações do Grupo Brasil Plural se dá através da adoção de uma estrutura descentralizada a fim de assegurar isenção de efetivos ou potenciais conflitos de interesses, bem como minimizar vulnerabilidades existentes e nossa exposição às ameaças referentes ao tema.

Como forma de ilustrar o acima exposto, a seguir, pode ser observada a organização estrutural e composição do Comitê do Grupo Brasil Plural no tocante à segurança das informações próprias e de terceiros, principalmente de clientes:



As responsabilidades pela definição, execução, gestão e monitoração da segurança da informação estão definidas como atribuições adicionais às funções que os colaboradores desempenham em suas respectivas áreas de atuação.

3.1. Papéis e Responsabilidades

Seguem abaixo transcritas as principais definições dos papéis e responsabilidade de colaboradores e áreas operacionais dentro de nossa empresa no que se refere à segurança de nossas informações.

Comitê de Segurança da Informação

- Deliberar sobre ações e decisões pertinentes à segurança das informações e incidentes;
- Conduzir o processo de investigação interna e apuração de causas e responsabilidades nos incidentes ou violações de segurança da informação;
- Tratar dos assuntos referentes ao tema em nível estratégico, tático e operacional;
- Reunir-se, sempre sob demanda e por e-mail, para tratar dos assuntos estratégicos, táticos e operacionais de segurança da informação, delegando responsabilidades e definindo alçadas de atuação;
- Aprovar escopo do Plano de Continuidade dos Negócios (“PCN”) do Grupo Brasil Plural;
- Submeter, para avaliação do Comitê Disciplinar mencionado no Código de Ética e Conduta, recomendações de penalidades e ações a serem tomadas para os casos não previstos neste Manual ou em quaisquer políticas internas referentes à segurança da informação;
- Manter atualização e debater regularmente sobre leis, normas e regulamentos referentes ao tema;
- Definir necessidades de investimentos e submeter à aprovação do Comitê Executivo;
- Definir programa de atuação e treinamento com estabelecimento de cronograma e prioridades; e
- Analisar e aprovar planos de ação, estratégias, políticas, procedimentos e controles de segurança da informação, coordenar a execução e acompanhamento de planos de ação, estratégias, políticas, procedimentos e controles de segurança da informação;
- Ministrando treinamento referente ao conteúdo deste Manual, sempre que necessário;
- Monitorar ativamente a observância dos dispositivos contidos neste Manual;
- Gerenciar as ações em segurança da informação física e lógica;
- Monitorar as atividades de administração de acessos físicos e lógicos;
- Assegurar existência de processo estruturado de informação e comunicação de incidentes e violações de segurança.

Área de Segurança

- Elaborar e atualizar regras e procedimentos referentes à segurança da informação;
- Monitorar a segurança dos recursos sob sua responsabilidade;
- Elaborar, implementar e analisar os indicadores de tecnologia para segurança da informação, tomando as ações necessárias para que estes se mantenham dentro dos padrões de segurança aceitáveis;

- Verificar e testar a vulnerabilidade nos sistemas do Grupo Brasil Plural;
- Convocar e coordenar as reuniões do Comitê; e
- Elaborar pauta, ata e divulgar, em conjunto com Compliance, as deliberações do Comitê;
- Sem prejuízo da revisão anual realizada pelo Administrativo, revisar os acessos físicos às dependências do Grupo Brasil Plural, trimestralmente, conforme procedimento interno definido para tal e respeitando-se a segregação de funções.

Compliance

- Participar ativamente das reuniões do Comitê de Segurança, como representante da área de Controles Internos;
- Analisar solicitações de acesso a sistemas, pastas na rede, inclusão em grupos de e-mail e *website*;
- Avaliar e recomendar liberação/vedação de arquivos a serem entregues a colaboradores, desligados ou não;
- Revisar e atualizar este Manual, no mínimo, anualmente ou quando necessário, em conjunto com as demais áreas integrantes do Comitê de Segurança da Informação;
- Aprovar termos de confidencialidade e responsabilidade para adesão de colaboradores ou terceiros visando atestar a responsabilização destes com as regras e padrões determinados pelo Grupo Brasil Plural;
- Elaborar e atualizar regras e procedimentos referentes à segurança da informação;
- Divulgar, em conjunto com o Agente de Segurança, as deliberações do Comitê.

Jurídico

- Definir e consolidar as provas e evidências necessárias para possibilitar a aplicação das penalidades previstas no Código de Ética e Conduta do Grupo Brasil Plural, assim como para a tratativa de eventuais demandas jurídicas;
- Auxiliar a Área de Gente, quando solicitado, na aplicação das penalidades constantes no Código de Ética e Conduta para as violações e incidentes de Segurança da Informação, elucidando questões de ordem jurídica que possam vir a ser suscitadas;
- Assegurar que os contratos celebrados com outras entidades e pessoas externas à empresa contenham, no mínimo, cláusulas que visem preservar a segurança das informações do Grupo Brasil Plural e, principalmente, de seus clientes;
- Monitorar para que as rescisões ou alterações em contratos não exponham o Grupo Brasil Plural a impactos negativos (de qualquer ordem) relacionados à segurança das informações; e
- Elaborar, quando solicitado, termos de confidencialidade e responsabilidade para adesão de colaboradores ou terceiros visando atestar a responsabilização destes com as regras e padrões determinados pelo Grupo Brasil Plural.

Área de Gente

- Comunicar imediatamente, ao Comitê de Segurança da Informação, informações sobre movimentações de colaboradores (transferências, demissões, desligamentos ou admissões) para que seus membros tomem as medidas necessárias de acordo com as diretrizes deste Manual e políticas internas aplicáveis;
- Checar informações pessoais e profissionais prestadas pelos colaboradores e informar tempestivamente ao Gestor e ao Comitê de Segurança da Informação;
- Aplicar, em conjunto com o Jurídico, as penalidades constantes no Código de Ética e Conduta para as violações e incidentes de Segurança da Informação;
- Acompanhar o comportamento dos colaboradores visando avaliar constantemente o grau de comprometimento com a segurança de nossas informações;
- Armazenar os termos de confidencialidade e responsabilidade de todos os colaboradores (inclusive temporários) do Grupo Brasil Plural;
- Manter relação atualizada de todos os profissionais atuantes na empresa, sejam funcionários ou terceiros;
- Em caso de observar, em entrevistas de desligamento, indícios de mau uso ou vazamento de informações do Grupo Brasil Plural (ou possibilidade), comunicar o fato tempestivamente à área de Compliance;
- No momento do desligamento de profissionais, recolher recursos e objetos de propriedade da empresa, tais como: crachás de identificação, chaves, documentos, mídias, computadores, celulares, dentre outros; e
- Zelar, no processo de admissão, pela contratação de profissionais com características e antecedentes pessoais que não indiquem possibilidade de comportamentos incompatíveis com o exercício da função, bem como valores e princípios éticos do Brasil Plural.

Risco

- Identificar, mensurar e controlar os diversos tipos de riscos sob sua gestão (mercado, operacional, crédito, liquidez e capital regulatório) envolvidos nas operações;
- Assegurar a confidencialidade de informações de clientes, dentro de sua alçada de atuação; e
- Elaborar, atualizar e gerenciar o PCN.

Processos

- Revisar e atualizar os perfis de acesso e acessos lógicos aos sistemas do Grupo Brasil Plural, no mínimo anualmente ou sempre que necessário, conforme procedimento interno definido para tal e respeitando-se a segregação de funções.

Administrativo

- Classificar os meios de informação não computadorizados que administra quanto à relevância para o Brasil Plural provendo condições mínimas necessárias de continuidade, disponibilidade e integridade desses (locais físicos, documentos, serviços e equipamentos);



- Providenciar adesão e armazenar, os termos de confidencialidade e responsabilidade de todos os fornecedores e prestadores de serviços terceirizados, alterando, quando necessário, a descrição de cargos;
- Contratar e atualizar apólice de seguro de bens e recursos do Grupo Brasil Plural de acordo com as determinações do Comitê de Segurança da Informação;
- Gerenciar ações e treinamentos necessários para os colaboradores integrantes da Brigada de Incêndio;
- Administrar serviços de manutenção e limpeza internos e terceirizados;
- Coordenar a recepção de clientes e visitantes;
- Gerenciar os serviços de expedição de documentos e correspondências;
- Garantir que os ambientes onde há compartilhamento de informações (Ex. salas de reunião e arquivos) tenham acesso restrito e controlado;
- Monitorar e tomar as ações necessárias para que recursos audiovisuais e físicos, disponíveis em salas de reunião e ambientes similares, como quadros, blocos de anotações, “datashow”, “flipchart”, lixeiras, estejam limpos, seguros e livres de qualquer informação relevante ou confidencial;
- Controlar entrada e saída de recursos físicos e lógicos da empresa;
- Revisar e atualizar os perfis de acesso e acessos físicos às dependências do Grupo Brasil Plural, no mínimo anualmente ou sempre que necessário, conforme procedimento interno definido para tal e respeitando-se a segregação de funções.
- Gerenciar os procedimentos inerentes à identificação e acesso físico de colaboradores, clientes e visitantes do Grupo Brasil Plural;
- Administrar os serviços de segurança patrimonial (proteção, utilização de câmeras, acessos físicos, fluxo de visitantes, dentre outras atividades); e
- Garantir a segurança e bom uso dos locais destinados para arquivo e armazenamento de documentos, mídias, dentre outros.

Tecnologia da Informação

- Classificar os meios de informação computadorizados que administra quanto à relevância para o Grupo Brasil Plural, provendo condições mínimas necessárias de continuidade, disponibilidade e integridade desses;
- Custodiar e administrar meios de informação informatizados, em uso ou de propriedade do Grupo Brasil Plural, tais como: *notebooks, netbooks, tablets, desktops*, servidores, redes de computadores, mídias, *softwares, hardwares*, aparelhos de telefone, sistemas de informação, bases e bancos de dados, periféricos, provedores de internet, *website*, intranet e outros relacionados com tecnologia;
- Homologar novos produtos de tecnologia (equipamentos, sistemas e softwares) de acordo com as regras e melhores práticas em segurança das informações;

- Definir critérios e condições (uso, horários, prevenção a acidentes e incidentes), bem como monitorar acesso e manutenção do *Data Center*;
- Implementar programas regulares de auditoria e avaliação de riscos de tecnologia com acompanhamento das áreas de Compliance, Risco Operacional e Auditoria Interna;
- Assegurar que exista um processo estruturado para registrar e informar os incidentes e violações de segurança em tecnologia da informação;
- Assegurar que existam processos para a identificação e verificação dos registros de atividades "logs" em todos os sistemas e recursos de tecnologia e dados;
- Seguir procedimentos rígidos que garantam a base tecnológica para recuperação de desastres e continuidade dos negócios do Grupo Brasil Plural;
- Testar e implementar as soluções tecnológicas de segurança, validadas e aprovadas pelo Comitê de Segurança da Informação, de acordo com este Manual, demais políticas internas, melhores práticas de mercado e as definições de negócio do Grupo Brasil Plural;
- Fornecer suporte técnico especializado a todos os colaboradores;
- Fornecer apoio técnico especializado aos Comitês de Segurança da Informação na elaboração do planejamento da estrutura e dos recursos que envolvam tecnologia;
- Fornecer informações sobre os projetos de sistemas e de tecnologia, em desenvolvimento, em manutenção e a desenvolver, para obter um parecer do Comitê de Segurança da Informação, no tocante às ameaças, vulnerabilidades e potenciais impactos negativos;
- Gerenciar processos de mudanças e de retorno à normalidade (na eventualidade de crises, incidentes e emergências que acarretem no acionamento do PCN);
- Assegurar a gravação telefônica dos ramais necessários e o *backup* diário de informações, mantendo em arquivo seguro e organizado durante os prazos legais e/ou internos;
- Zelar pelo uso e segurança, bem como o armazenamento interno e externo das mídias de *backup* durante os prazos internos definidos e os dispostos em leis, normas e regulamentos;
- Manter a confidencialidade das informações que tenham acesso; e
- Garantir a confidencialidade, disponibilidade e integridade das informações armazenadas nos equipamentos, sistemas e bases de dados do Grupo Brasil Plural.

Cadastro

- Cadastrar clientes nos sistemas internos e externos;
- Garantir confidencialidade das informações de clientes;
- Armazenar de forma segura e organizada os documentos cadastrais dos clientes do Grupo Brasil Plural, tanto interna quanto externamente;
- Assegurar acesso restrito e controlado ao local de arquivamento interno e manuseio de documentos de clientes;

- Avaliar e monitorar as ações de prestadores de serviços terceirizados que desempenhem suas atividades juntamente com a equipe de Cadastro do Brasil Plural, no tocante a guarda de arquivos e documentos de clientes;
- Submeter para análise do Jurídico, documentos passíveis de revisão (Ex. contratos, acordos, etc);
- Comunicar, à área de Compliance, situações onde existam vulnerabilidades quanto à proteção dos recursos e informações do Grupo Brasil Plural e de clientes.

Auditoria Interna

- Avaliar as decisões do Comitê observando eventuais desvios na eficácia dos controles atualmente executados;
- Testar e identificar, obedecendo ao plano de auditoria interna, falhas nas regras e controles estabelecidos pelo Comitê de Segurança; e
- Cumprir o cronograma anual de auditoria de sistemas, reportando eventuais pontos de atenção identificados ao Comitê de Segurança.

Áreas Comerciais e de Relacionamento com Clientes

- Adicionalmente às responsabilidades de atendimento, prospecção (incluindo, principalmente, conhecer o cliente conforme as regras internas e melhores práticas), cadastro, captação, atualização cadastral e fidelização de clientes, estas áreas do Grupo Brasil Plural devem assegurar a confidencialidade, integridade e disponibilidade das informações e documentos pessoais de clientes sob sua responsabilidade, conforme as políticas e diretrizes internas, bem como as orientações das áreas de Cadastro e Compliance; e
- Comunicar, à área de Compliance, situações onde existam vulnerabilidades quanto à proteção dos recursos e informações do Grupo Brasil Plural e de clientes.

Membros do Comitê Executivo e Diretoria

- Disseminar a importância do cumprimento de todo o conteúdo disposto neste Manual, Código de Ética e Conduta ou demais políticas e diretrizes internas, bem como tomar conhecimento quanto à observância das regras através da revisão e aprovação de relatórios e pareceres, participação em Comitês sobre o tema, avaliando ações e investimentos necessários, seguindo continua e ativamente os padrões e regras definidos, dentre outros.

Gestores das Áreas

- Identificar arquivos, documentos e recursos relevantes sob sua responsabilidade que necessitam de classificação e tratamento;
- Comunicar, previamente à Área de Gente, situações referentes à movimentação de pessoal (transferências, promoções, demissões, desligamentos, licenças, férias, suspensões ou admissões);
- Reportar imediatamente para Compliance quaisquer suspeitas de não conformidades com as regulamentações e definições constantes neste Manual, no Código de Ética e Conduta ou

demais políticas e diretrizes internas, bem como a percepção de ações ou acontecimentos fora das condições normais de operação do Grupo Brasil Plural;

- Apoiar, implementar e cumprir, dentro de sua esfera de responsabilidade, as políticas, diretrizes, procedimentos, padrões e demais regulamentações às quais a Plural e seus colaboradores devem seguir e respeitar;
- Assumir a responsabilidade de proprietário das informações de sua área ou quando a classificação da informação assim exigir; e
- Comunicar, à área de Compliance, situações onde existam vulnerabilidades quanto à proteção dos recursos e informações do Grupo Brasil Plural e de clientes.

Demais Colaboradores

- Respeitar e cumprir de forma ampla e irrestrita todo o conteúdo disposto neste Manual, no Código de Ética e Conduta e demais políticas e diretrizes;
- Ter ciência de que todas as informações geradas, acessadas, processadas, utilizadas ou armazenadas em qualquer meio ou sistema de informação, devem ser relacionadas às suas atividades profissionais e poderão ser monitoradas e auditadas pelo Grupo Brasil Plural, não cabendo nenhuma expectativa de privacidade do colaborador;
- Informar ao Jurídico sobre eventuais processos que venham a ser instaurados contra si;
- Reportar imediatamente, para a área de Compliance, quaisquer violações ou incidentes de segurança da informação, bem como situações não enquadradas nas condições normais de operação e atuação do Grupo Brasil Plural; e
- Participar dos treinamentos e disseminar a importância de todos agirem com responsabilidade no tocante ao tratamento das informações do Grupo Brasil Plural e de seus clientes.

4. Classificação das Informações

No Grupo Brasil Plural, dividimos nossas informações em dois grandes grupos:

- Informações de clientes;
- Informações corporativas (incluindo informações de produtos e serviços).

A segurança efetiva de nossas informações deve se basear em critérios e controles rígidos de tratamento que serão abordados a seguir, e visando maximizar a alocação dos recursos e esforços do Grupo Brasil Plural, classificamos nossas informações nas seguintes categorias:

4.1. Relevância e Integridade

- **Confidencial** – é a informação que pode causar danos e prejuízos gravíssimos para o Grupo Brasil Plural e seus clientes. Deve ser totalmente preservada, em seu estado original, durante todo o período de necessidade de armazenamento.

Quanto a este tipo de informação, algumas regras básicas devem ser observadas:

- É vedada a divulgação fora da empresa ou mesmo internamente para pessoas que não necessitem de seu conhecimento para o exercício de suas funções (*Need to Know Policy*);
 - Acesso é exclusivo ao reduzido número de colaboradores autorizados, geralmente membros do Comitê Executivo, Diretoria, Sócios e Gestores;
 - Deve ser armazenada em local de acesso restrito e seguro;
 - Quaisquer informações de clientes devem ser classificadas e tratadas como estritamente confidenciais assim como os relatórios de fiscalização, auditoria, *rating*, e de órgãos reguladores ou fiscalizadores.
- **Restrita** – trata-se da informação que, se divulgada ou acessada por pessoas não autorizadas, pode acarretar em danos e prejuízos moderados ou graves para o Grupo Brasil Plural. Deve ser totalmente preservada, em seu estado original, durante todo o período de necessidade de armazenamento.

Divulgação ou acesso restrito, somente com autorização prévia e formal da Diretoria de Meios e da área de Compliance.

- **Interna** – informação com acesso autorizado somente aos colaboradores que a necessita para o exercício pleno de suas funções. Os danos ou prejuízos causados pela divulgação não autorizada são de impacto brando ou moderado para o Grupo Brasil Plural. Deve, ainda, ser passível de controles básicos a fim de evitar que sua integridade seja abalada.

A divulgação somente deve ocorrer com validação da área de Compliance.

- **Pública** – esta é de conhecimento irrestrito e pode ser divulgada fora da empresa, com anuência da área de Compliance e desde que sejam respeitadas as regras dispostas neste Manual e demais políticas e diretrizes internas.

4.2. Disponibilidade

Nesta categoria, as informações são classificadas quantitativamente permitindo a formalização de um indicador quanto ao seu tempo máximo de indisponibilidade aceitável (“MAO” – *maximum acceptable outage*).

Periodicamente será mensurado qual o período máximo que a informação poderá ficar indisponível antes de começar a impactar significativamente os objetivos operacionais ou a própria continuidade da empresa.

Esta informação é vital para o sucesso das estratégias de continuidade de negócios do Grupo Brasil Plural.

4.3. Retenção

Prazo que a informação deverá ser armazenada, bem como quando e como poderá ser descartada ou destruída.

O Grupo Brasil Plural adota como período mínimo de guarda o prazo definido pelas leis e normas aplicáveis às nossas atividades e, em alguns casos, define períodos de retenção mais restritivos que os próprios órgãos reguladores, conforme classificação prévia da informação.

5. Tratamento e proteção dos ativos de informação

A seguir, estão dispostas regras e diretrizes não exaustivas quanto à proteção e tratamento dos ativos de informação do Grupo Brasil Plural e quaisquer dúvidas ou esclarecimentos devem ser imediatamente direcionados aos membros dos Comitês de Segurança da Informação anteriormente mencionados.

5.1. Guarda de Informações

- Documentos classificados como confidenciais ou restritos, principalmente de clientes, devem ficar armazenados em locais (físicos ou lógicos) de acesso restrito, seguros e organizados quando não estiverem sendo utilizados;
- Locais destinados ao armazenamento de informações de clientes e demais informações corporativas restritas ou confidenciais devem ser monitorados através de câmeras de segurança, registro/análise de “logs” e controle de acesso rigoroso;
- O período de armazenamento de informações, antes do descarte, deve respeitar os períodos legais aplicáveis ou de políticas e diretrizes internas mais restritivas;
- Quaisquer informações lógicas somente devem ser armazenadas na rede corporativa, ou seja, é vedada a gravação de arquivos no disco rígido local (Diretório “C:”) e, ainda, em qualquer tipo de mídia sem análise e autorização da área de Compliance;
- O e-mail não deve ser utilizado primariamente para guarda de informações;
- Os locais de arquivamento externo, seja de mídias ou documentos físicos, devem ter contrato formalizado, com acordos de SLA (Acordo de Nível de Serviço) definidos e serem objeto de processo de *due diligence* com visitas periódicas, conforme o caso;
- Documentos de qualquer classificação “esquecidos” nas impressoras ou em locais não apropriados serão identificados e os colaboradores passíveis das penalidades internas cabíveis; e
- O envio e recebimento de informações e documentos em meio físico de/para locais externos devem ser necessariamente protocolados e controlados quanto à entrada e saída do Brasil Plural.

5.2. Acesso Físico e Lógico

A credencial de acesso a qualquer meio lógico ou físico trata-se de um importante mecanismo de controle e segurança de nossos ativos de informação. As áreas responsáveis, conforme atribuições descritas no item 3 deste Manual, realizarão a revisão dos perfis e dos acessos físicos e lógicos no mínimo anualmente ou sempre que necessário, de acordo com o procedimento interno definido para tal e respeitando-se a segregação de funções. As não conformidades eventualmente detectadas durante esses processos poderão ser discutidas pelo Comitê de Segurança da Informação.

Acesso Lógico

Os perfis de acesso devem respeitar a segregação de funções estabelecida pelas normas vigentes e regras internas;

- O gestor deve solicitar, no momento da contratação do novo colaborador ou da movimentação de área do colaborador antigo, os acessos necessários aos diversos sistemas do Grupo Brasil Plural.
- Os colaboradores desligados deverão ter seus acessos revogados no momento imediato do desligamento;
- Todo profissional que tenha acesso aos sistemas de informação do Grupo Brasil Plural é responsável por tomar todas as medidas necessárias a fim de impedir o acesso não autorizado;
- Adicionalmente à regra lógica de bloqueio automático das estações de trabalho, todos devem travar o acesso aos seus computadores (CTRL+ALT+DEL) quando se ausentarem do local físico de trabalho, independentemente do período de ausência.

Acesso Físico

- O crachá de acesso ao prédio e dependências internas é pessoal e intransferível;
- As demais formas de acesso físico (Ex. biometria) somente deverão ser concedidas para os colaboradores que necessitarem para o exercício das funções e conforme orientação da área de Compliance;
- Todos os crachás possuem níveis de acesso diferenciados conforme cargo e/ou função a fim de evitar conflito de interesses e acesso não autorizado de informações;
- A recepção do Grupo Brasil Plural deve registrar a entrada e saída de terceiros ou visitantes independentemente dos critérios de identificação do condomínio;
- O registro supracitado deve conter, no mínimo, a data, horário, tipo da visita (cliente, particular ou prestação de serviço) e o colaborador do Grupo Brasil Plural responsável;
- Qualquer terceiro ou visitante deve aguardar, obrigatoriamente, em sala de espera ou de reunião;
- O crachá do visitante deve ser apenas para identificação e sem qualquer tipo de acesso permitido, salvo nos casos autorizados pela Diretoria de Meios e conforme orientação de Compliance;
- Arquivo com cadastro de clientes, Data Center, área de Research, Financeiro dentre outras são de acesso restrito às pessoas destas áreas e demais profissionais autorizados pelo Comitê Executivo.

Política de Senhas

Conforme anteriormente mencionado, cumpre-nos ressaltar que a senha de acesso a qualquer meio lógico ou físico trata-se de um dos mais básicos e importantes mecanismos de segurança de nossas informações.

A fim de assegurar as melhores práticas relacionadas a este tema, seguem abaixo algumas das diretrizes que devem ser observadas por todos:



- A senha deve ser memorizada e de uso pessoal e intransferível;
- O eventual uso ou acesso indevido é de total responsabilidade do detentor e titular da senha que deve tomar todos os cuidados necessários para salvaguardá-la;
- A senha de acesso aos sistemas internos deverá seguir os critérios definidos pelo Comitê de Segurança da Informação;
- O compartilhamento de senhas somente será permitido em casos de indisponibilidade para uso individual e se aprovado prévia e formalmente pelo Comitê de Segurança da Informação;
- Toda e qualquer senha, de acesso físico ou lógico, deverá ser imediatamente bloqueada em casos de desligamento e/ou demissão,;
- Especificamente com relação à senha de acesso à rede corporativa, a política é a seguinte:
- Deve ter, no mínimo, 6 (seis) caracteres e atender, no mínimo, a 3 dos 4 grupos de caracteres abaixo citados:
 - A. Letras maiúsculas (de A a Z);
 - B. Letras minúsculas (de a a z);
 - C. Algarismos (de 0 a 9); e
 - D. Caracteres não-alfabéticos (Ex. !, #, @, #, %).
- Deverá ser alterada, compulsoriamente, a cada 45 (quarenta e cinco) dias;
- Não pode ser igual ou similar às 6 (seis) últimas utilizadas;
- Não pode conter seu nome completo ou o de sua conta;
- Em hipótese alguma será concedida senha de acesso a outro funcionário que não seja o próprio usuário; e
- Ao receber a “nova” senha, o usuário deverá, obrigatoriamente, alterá-la no primeiro acesso seguindo os critérios acima citados.

5.3. Mídias e Recursos Portáteis

- Mídias e recursos portáteis ou móveis devem ser controlados e registrados;
- Os funcionários usuários de recursos portáteis (incluindo telefones celulares, conforme disposto na “CPP.005 – Celular Corporativo”) devem comprovar, através de um termo de responsabilidade, que tomarão todos os cuidados no transporte e utilização destes equipamentos conforme orientação da área de Tecnologia da Informação; e
- Nenhum dispositivo ou equipamento eletrônico para transmissão, armazenamento ou manuseio de dados, tais como: CD, DVD, máquina fotográfica, celular, HD portátil, *pen drive*, *tablet*, *memory card* ou similar deve ser conectado ou utilizado nas instalações do Grupo Brasil Plural sem análise e aprovação prévia do Comitê de Segurança da Informação.

5.4. E-mail e Telefonia

Conforme disposto em nosso Código de Ética e Conduta, o Grupo Brasil Plural fornece sistemas de comunicação eletrônica ou por voz, tais como e-mail, telefones fixos e celulares, para fins profissionais.

Em relação ao uso do e-mail e comunicação por voz, todos devem observar as seguintes regras abaixo transcritas:

- O uso para fim pessoal deve ser de caráter resumido e objetivo. Todavia, é proibido o uso para ganho pessoal, malas diretas, “correntes”, ameaças, assédio, entretenimento, dentre outros considerados impróprios ou ilegais;
- O correio eletrônico não pode ser utilizado, sem aprovação do Comitê, para envio ou recepção de mensagens que contenham arquivos executáveis, macros ou sequências de comandos, explícitas ou implícitas, ou ainda outros mecanismos que possam conter vírus e, portanto, possam causar dano físico ou lógico aos equipamentos do Grupo Brasil Plural ou de seus destinatários;
- E-mails de remetentes ou assuntos desconhecidos não devem ser abertos em nenhuma hipótese e imediatamente reportados às áreas de Compliance e Tecnologia da Informação;
- O uso do webmail corporativo e acesso remoto à rede e arquivos somente são concedidos a alguns colaboradores e mediante aprovação prévia do Comitê;
- Todos os arquivos que são enviados e recebidos devem passar por um “filtro de e-mail” controlado e monitorado;
- Atendimentos a clientes e realização de operações devem ser realizados somente através de ramais gravados;
- Os serviços de e-mail providos pelo Grupo Brasil Plural possuem algumas restrições que visam manter a qualidade e a disponibilidade do serviço e da infra-estrutura que compõe a área de TI. São elas: (i) Tamanho máximo de arquivo em anexo: 35MB (35 Megabytes), salvo raras exceções, que possuem configuração compatível com tamanho máximo de 10MB; (ii) Sistemas de Anti-Vírus e Anti-Spam são atualizados diariamente e apagam os e-mails que contenham vírus e colocam em quarentena os que forem classificados como spam; (iii) Limite máximo de 25 destinatários; (iv) Capacidade máxima de 50G de armazenamento de Caixa-Postal, salvo raras exceções, que possuem configuração compatível com capacidade máxima de 5G.

5.5. Uso da Internet

O uso da Internet pelos empregados do Grupo Brasil Plural é permitido e encorajado desde que seu uso seja aderente aos objetivos e atividades fins do negócio da Empresa. Entretanto, o Grupo Brasil Plural tem uma política para o uso da Internet desde que os funcionários/colaboradores assegurem que cada um deles:

- Siga a legislação corrente (sobre pirataria, pedofilia, ações discriminatórias.);
- Uso razoável da Internet, sempre prezando pelo bom senso quanto aos sites acessados e tempo de utilização; e
- Não crie riscos desnecessários para o negócio do Grupo Brasil Plural.

É estritamente proibido e inaceitável

Concorrentemente ao descrito acima, será considerado totalmente inaceitável tanto no uso quanto no comportamento dos empregados:

- visitar sites da Internet que contenha material obsceno e/ou pornográfico;
- usar o computador para executar quaisquer tipos ou formas de fraudes, ou software/musica pirata;
- usar a Internet para enviar material ofensivo ou de assédio para outros usuários;
- baixar (download) de software comercial ou qualquer outro material cujo direito pertença a terceiros (copyright), sem ter um contrato de licenciamento ou outros tipos de licenciamento;
- atacar e/ou pesquisar em áreas não autorizadas (Hacking);
- criar ou transmitir material difamatório;
- executar atividades que desperdice os esforços do pessoal técnico ou dos recursos da rede;
- introduzir de qualquer forma um vírus de computador dentro da rede corporativa.

Monitoramento

O Grupo Brasil Plural reafirma que o uso da Internet é uma ferramenta valiosa para seus negócios. Entretanto, o mau uso dessa facilidade pode ter impacto negativo sobre a produtividade dos funcionários e a própria reputação do negócio. Em adição, todos os recursos tecnológicos do Grupo Brasil Plural existem para o propósito exclusivo de seu negócio. Portanto, a empresa se dá ao direito de monitorar o volume de tráfego na Internet e na Rede, juntamente com os endereços web visitados.

5.6. Utilização de Software

Toda instalação de software deve ser feita pela área de TI e todos os softwares e aplicativos devem ser homologados e licenciados. Softwares instalados pela Internet, CD-ROM ou qualquer outro meio de mídia magnética, diretamente pelo usuário ou por terceiros em qualquer equipamento ligado à rede do Grupo Brasil Plural, sem conhecimento do departamento de TI, e não considerado de interesse do Brasil Plural, ou que infrinjam as regras desta política, podem ser desinstalados pela TI sem aviso prévio.

A utilização de softwares fora dos padrões (como navegadores), bem como softwares livres ou temporários e sendo a sua utilização necessária, deverão ser tratados como exceções e deverão ser autorizados pelo responsável pela administração da rede e sempre instalados ou acompanhados pelo pessoal técnico do departamento de TI, desde que não prejudique o funcionamento de sistemas ou inflijam alguma regra, avisos ou boletins de segurança. Os mesmos deverão ser revisados trimestralmente e não contarão com suporte da TI.

A utilização de softwares não licenciados é considerada uma Não-Conformidade Gravíssima e acarretará punições ao funcionário ou colaborador, em qualquer nível, do Grupo Brasil Plural.

Todo parque tecnológico é mantido nas versões mais atuais desde que compatíveis com diversos Recursos Tecnológicos existentes e livres de falhas e erros que prejudiquem o uso em condições aceitáveis. A atualização é feita após análise de impacto realizada pelo departamento de TI.

5.7. Descarte de Informações

Toda informação que não necessite de sua manutenção em arquivos deve ser descartada, depois de decorrido o prazo legal, somente através de máquinas fragmentadoras (neste caso, somente para as classificadas como confidenciais ou restritas) e/ou conforme orientação da área de Compliance.

Adicionalmente à vedação de uso do e-mail para armazenamento primário de mensagens e arquivos (vide item “V.1 – Guarda de Informações”), ressaltamos que todos os colaboradores devem adotar a prática de apagar mensagens (principalmente as que contenham arquivos anexados) antigas ou desnecessárias.

5.8. Comunicação Verbal

Os colaboradores devem adotar cuidados especiais para evitar o comprometimento da segurança das informações através da comunicação verbal.

- É vedado tratar sobre assuntos confidenciais, restritos ou internos em locais onde estejam presentes pessoas não autorizadas. Adicionalmente, recomenda-se fortemente não gravar mensagens com conteúdo confidencial ou restrito em secretárias eletrônicas, caixas postais e afins; e
- Informações classificadas como confidenciais não devem ser comunicadas por telefone.

5.9. Incidentes de Segurança

Em caso de ocorrência de um vazamento de informações ou incidente de segurança, o colaborador deve registrar e comunicar o fato imediatamente à área de Compliance ou a algum membro do Comitê de Segurança das Informações.

6. Resumo das principais vedações

É proibido aos usuários da rede:

- Acessar, copiar ou armazenar programas de computador ou qualquer outro material (músicas, fotos e vídeos) que violem a lei de direitos autorais, bem como aqueles de conteúdo ilegal, pornográfico, discriminatório, homofóbico, racista, de apologia a crimes, dentre outros;
- Passar-se por outra pessoa ou esconder, por qualquer meio, a própria identidade quando utilizar os recursos computacionais ou quaisquer outros de propriedade do Brasil Plural, colocados à disposição do colaborador em razão do exercício de sua função;
- Usar ou divulgar informações confidenciais obtidas para benefícios pessoais (oportunidades de emprego, investimentos, dentre outros) mesmo após o término de seu vínculo com o Grupo Brasil Plural;
- Alterar os sistemas padrões, sem autorização;
- Divulgar quaisquer informações confidenciais para concorrentes e/ou qualquer pessoa não ligada às atividades da Empresa;



- Efetuar qualquer tipo de acesso ou alteração não autorizada a dados dos recursos computacionais pertencentes à Empresa;
- Violar os sistemas de segurança dos recursos computacionais, no que tange à identificação de usuários, senhas de acesso, fechaduras automáticas, sistemas de alarme e demais mecanismos de segurança e restrição de acesso;
- Utilizar acesso através de modem, ou qualquer outra forma de conexão não autorizada, quando conectado às redes instaladas nas dependências do Grupo Brasil Plural;
- Acessar e-mail pessoal e serviços de mensagens instantâneas não autorizadas formalmente pelo Comitê de Segurança da Informação;
- Utilizar o telefone do Grupo Brasil Plural para assuntos pessoais durante período de tempo não razoável;
- Criar blogs ou comunidades na Internet, ou qualquer ambiente virtual semelhante, fazendo uso, sem autorização expressa, da logomarca ou do nome do Grupo Brasil Plural;
- Fazer uso do telefone celular e outros meios de comunicação e gravação particulares dentro das dependências do Grupo Brasil Plural nos locais não autorizados; e
- Uso ou instalação de softwares não licenciados e sem autorização da área de Tecnologia da Informação.

7. Treinamento

Todos os colaboradores do Brasil Plural deverão, além de aderir a este Manual, receber, periodicamente, treinamentos e materiais educativos que visem, principalmente, a conscientização e reciclagem de conhecimento de todos sobre o tema.

Novos colaboradores são submetidos obrigatoriamente a um treinamento inicial acerca de suas funções e responsabilidades quanto ao assunto, durante o Programa de Integração coordenado pela área de Gente. Essa mesma área efetuará o registro e o controle formal de presença, indicando a frequência e o tipo de treinamento ministrado, de modo a possibilitar o planejamento e a manutenção dos níveis mínimos de segurança.

Todos os treinamentos são preferencialmente ministrados por profissionais internos capacitados e diretamente ligados aos controles de segurança de informação do Grupo Brasil Plural.

8. Considerações finais

Todos os colaboradores devem atestar a leitura e perfeita compreensão deste documento e suas posteriores alterações.

Em casos de dúvidas ou esclarecimentos sobre o conteúdo deste Manual ou sobre a aplicação do mesmo em relação a algum assunto específico, os participantes do Comitê de Segurança da Informação deverão ser consultados.

O descumprimento de alguma regra desta política será considerado como falta Grave, conforme disposto no Código de Ética e Conduta do Grupo Brasil Plural ou de acordo com análise de decisão do Comitê.



www.brasilplural.com

Rua Surubim, 373
1º andar - Vila Olímpia
CEP: 04571-050
Tel: 55 11 3206 8000
São Paulo - SP

Praia de Botafogo, 228
9º andar - Botafogo
CEP: 22250-906
Tel: 55 21 3923 3000
Rio de Janeiro - RJ

Rua Mostardeiro, 322
7º andar - Independência
CEP: 90430-000
Tel: 55 51 3455 9300
Porto Alegre - RS

N.Y. Affiliate
Brasil Plural Securities LLC
545 Madison Av. 8th Floor - 10022
Tel: 1 212 388 5600
New York - NY