Política de Segurança Cibernética

Janeiro de 2020

Elaboração: Comitê de Segurança da Informação

Aprovação: Diretoria Executiva

Classificação: Interno

Índice

1. OBJETIVO

Esta política tem por objetivo estabelecer os fundamentos associados ao processo de segurança cibernética definidos com base em princípios e diretrizes que buscam assegurar a confidencialidade, a integridade e a disponibilidade de dados e dos sistemas de informação, em conformidade com a Resolução CMN n° 4.658, de 26 de abril de 2018.

Este documento dará as diretrizes para a criação de normas e procedimentos visando a proteção cibernética do Grupo Brasil Plural, observando a natureza das suas operações, a complexidade dos produtos, serviços, atividades e processos, bem como o seu porte, perfil de risco, modelo de negócio e a sensibilidade dos dados e das informações sob responsabilidade da instituição, visando prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

2. ABRANGÊNCIA

Esta política é aplicada para as Instituições do conglomerado Brasil Plural, partes interessadas e a quem possa tratar ou transmitir dados ou informações das instituições que fazem parte do conglomerado.

3. DEFINIÇÕES

Para efeitos desta política, define-se Segurança Cibernética como um conjunto de práticas que protegem as informações armazenadas nos computadores, aparelhos de computação e smartphones e a transmissão destes dados através das redes de comunicação incluindo a internet.

No arcabouço de Segurança Cibernética alguns conceitos são essenciais para a compreensão do processo, assim definidos:

i. **Informações Confidenciais**: São informações confidenciais aquelas, não disponíveis ao público, que possam identificar dados pessoais ou patrimoniais, informações que possam ser objeto de acordo de confidencialidade celebrado com terceiros e ações estratégicas cuja divulgação possa prejudicar a gestão dos negócios ou reduzir vantagens competitivas.

ii. **Ataques Cibernéticos**: Os ataques cibernéticos mais comuns, podem ser realizados através de software maliciosos que são desenvolvidos para corromper computadores e redes de dados, que podem ser realizados através de métodos de manipulação para obtenção de informações confidenciais, como senhas e dados pessoais, ou que possa visar a negação ou atraso de acessos aos serviços ou sistemas da instituição.

iii. **Incidente de Segurança da Informação**: Um incidente de segurança da informação pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança dos

sistemas de computadores ou das redes de computadores, que pode comprometer a Confiabilidade, Integridade e/ou Indisponibilidade das informações.

4. Diretrizes

Em linha com o escopo desta política, seguem abaixo transcritas as diretrizes gerais para a proteção.

a-) Toda e qualquer informação que estiver sobre o domínio do Grupo Brasil Plural ou sob a guarda de qualquer um de seus colaboradores e parceiros é de propriedade, uso exclusivo e mantido pela "Política de Segurança Cibernética" e "Política de Segurança da Informação".

Toda informação gerada pelo Grupo Brasil Plural é de uso exclusivo da mesma, não sendo permitida a sua divulgação para entidades externas;

A informação só poderá ser divulgada a entidades externas mediante a autorização do responsável pela informação;

Toda a informação deverá ser classificada e controles deverão ser estabelecidos para garantir a sua confidencialidade, disponibilidade e integridade.

b-) Todos os colaboradores e parceiros do Grupo Brasil Plural, incluindo a alta administração e todo o corpo gerencial, devem estar cientes sobre a Política de Segurança Cibernética e Política de Segurança da Informação, devem receber treinamento adequado para utilizar as informações da organização.

Para tal, mecanismos de disseminação da cultura de segurança devem ser aplicados;

Periodicamente os Colaboradores devem ser conscientizados e avaliados;

Os Colaboradores devem ser capacitados para desenvolver suas atividades com segurança, para tanto os colaboradores que manuseiam informações sensíveis e críticas para o negócio bem como a equipe de TI devem receber treinamento adequado;

Processos disciplinares rigorosos devem ser aplicados aos Colaboradores que violarem a Política de Segurança Cibernética e a Política de Segurança da Informação;

Prestar informações aos clientes e usuários sobre as precauções na utilização de produtos e serviços financeiros e divulgar ao público o resumo contendo as linhas gerais da Política de Segurança Cibernética e Política de Segurança da Informação.

c-) Todos os ativos do Grupo Brasil Plural devem ser classificados e protegidos de acordo com a sua importância para o negócio tendo como base uma gestão contínua de risco e impacto.

Um processo de gerenciamento de riscos e impacto de segurança cibernética deverá ser estabelecido com o objetivo de levantar e gerenciar os riscos e impactos de cibersegurança que o

Grupo Brasil Plural possa estar exposto. A equipe de Segurança da Informação deverá ser responsável por essa atividade na organização;

Um Comitê de Segurança da Informação deve ser estabelecido para deliberar sobre as ações de tratamento dos risos levantados;

Para cada ativo deverá ser eleito um responsável que deverá estabelecer o nível de proteção adequada, o mesmo deverá definir qual (is) entidade(s) poderá (ão) manipular determinado ativo, e quais os níveis de privilégio.

d-) Todas as informações e os ativos que a comportam, devem ser gerenciados e os acessos controlados.

O acesso lógico a informação deve ser controlado. Deverá existir um processo para concessão, revogação e alteração de acessos e privilégios, que envolva o dono da informação autorizando as permissões;

Todo Colaborador/Parceiro deve ter acesso aos recursos e informações somente com os privilégios mínimos e necessários para desenvolver suas atividades;

Trilhas de auditoria devem ser implementadas para reconstituições das ações.

e-) Todos os incidentes relevantes relacionados com o ambiente cibernético deverão ser gerenciados.

Em casos de ocorrência de um incidente de segurança da informação, a tratativa poderá ser conduzida das seguintes formas:

Incidentes comportamental deverá ser reportado para a área de Compliance ou a para o Comitê de Segurança da Informação, que analisará caso a caso e adotará as medidas cabíveis conforme estabelecido no Código de Ética e de Conduta;

Incidente técnico relacionado a qualquer tipo de ameaça ou vulnerabilidade deverá ser tratado através de procedimento técnico que tem como papel fundamental agir e mitigar o incidente o mais rápido possível;

Ações proativas que visem prevenir a ocorrência de incidentes cibernéticos deverão ser implementadas;

A área de Segurança da Informação é responsável por realizar a gestão de incidente cibernéticos do Grupo Brasil Plural;

Deverá ser estabelecido um Plano de Ação e de Resposta a Incidentes o qual deverá contar com as rotinas, os procedimentos, os controles e as tecnologias a serem utilizadas na prevenção e nas respostas aos incidentes, em conformidade com as diretrizes da política de segurança cibernética;

O Plano de Ação e de Resposta a Incidentes deverá ser aprovado pela Diretoria Executiva do Grupo Brasil Plural;

Todos os incidentes classificados como graves ou relevantes deverão conter relatórios com as seguintes informações:

Descrição do incidente;

Ações tomadas para conter o incidente;

Avaliação do impacto ou dano causado pelo incidente;

Ações tomadas para recuperação dos danos causados;

Descrição das possíveis causas do incidente.

Ações de prevenção deverão ser implementadas para que o incidente não volte a ocorrer;

O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes, devem abranger também as empresas parceiras prestadoras de serviço;

De acordo com a resolução 4658, de 26 de abril de 2018 deverá ser elaborado um relatório anual sobre a implementação do plano de ação e de resposta a incidentes com data base de 31 de dezembro, o mesmo deverá ser submetido ao Comitê de Risco e apresentado à Diretoria Executiva até 31 de março do ano seguinte ao da data-base; e

Iniciativas de compartilhamento de informações sobre os incidentes relevantes com outras instituições financeiras devem ser fomentadas.

f-) Todos os processos importantes ou de grande relevância para o Grupo Brasil Plural devem ter planos de continuidade formalizados, revisados e testados de acordo com a necessidade do negócio ou seu nível de importância.

Todos os processos devem ser mapeados, e avaliados e classificados como críticos ou não para a organização;

Planos de continuidade e desastre deverão ser elaborados com os cenários definidos na avalição de risco e análise de impacto. Os planos devem ser e revisados periodicamente;

Backups das informações devem ser realizados, testados regularmente e estar disponíveis para atender em qualquer situação emergencial;

Teste de continuidade de negócios devem ser realizados periodicamente levando em consideração os cenários de indisponibilidade ocasionados por incidentes e mapeados no plano de continuidade de negócios.

g-) Todas as informações do Grupo Brasil Plural devem estar protegidas das ameaças virtuais.

Ferramentas de prevenção e detecção de códigos maliciosos (vírus, cavalos-de-tróia, etc.) devem ser implementadas para proteger a integridade e disponibilidade das informações;

Ferramentas de detecção e prevenção de ataques virtuais devem ser implementadas para proteger a integridade, disponibilidade e confidencialidade das informações;

Deverá existir um processo de "Gestão de Vulnerabilidades" no ambiente tecnológico composto por procedimentos e controles que visem a reduzir as vulnerabilidades as quais o Grupo Brasil Plural possa estar exposto, tais como:

Realização periódica de testes e varreduras para detecção de vulnerabilidades;

Realização de testes de invasão.

Controles que visão a prevenção de vazamento de informações devem ser implementados.

A autenticação e criptografia devem ser implementados como controles para garantir a segurança das informações no ambiente cibernético.

Para o desenvolvimento ou aquisição de software e novas tecnologias, devem ser observados os controles de segurança cibernética em todo o ciclo de desenvolvimento para criar de aplicações e sistemas.

h-) Os fornecedores e parceiros de negócios do Grupo Brasil Plural devem seguir os mesmos níveis de controles que o Grupo Brasil Plural implementa.

Deverá ser estabelecido um processo para avaliação de fornecedores e parceiros de negócio antes de firmar um contrato, para levantar os pontos de controle que o fornecedor ou parceiro de negócio deve ter;

O Grupo Brasil Plural deve estabelecer em seus contratos os controles que os seus fornecedores ou parceiros de negócios devem estabelecer;

O Grupo Brasil Plural deve realizar auditorias em seus fornecedores e parceiros de negócio para verificar a efetividade dos controles estabelecidos.

5. ESTRUTURA DE DOCUMENTOS

A estrutura de documentos que representam a Segurança da Informação, Segurança Cibernética e Privacidade é composta de seguinte forma:

(i) Políticas;

(ii) Normas;

(iii) Procedimentos; e

(iv) Manuais e Recomendações.

5.1. Políticas:

Regras de alto nível que representam os princípios básicos que a organização resolveu incorporar a sua gestão de acordo com a visão estratégica da alta direção leis e regulamentações. Servem como base para que as normas e os procedimentos sejam criados e detalhados.

5.2. Normas:

Especificam no plano tático, por assim dizer, as escolhas tecnológicas e os controles que deverão ser implementados para alcançar a estratégia definida nas diretrizes.

5.3. Procedimentos:

Detalham, no plano operacional, as configurações de um determinado produto ou funcionalidade que devem ser feitas para implementar os controles e tecnologias estabelecidas nas normas.

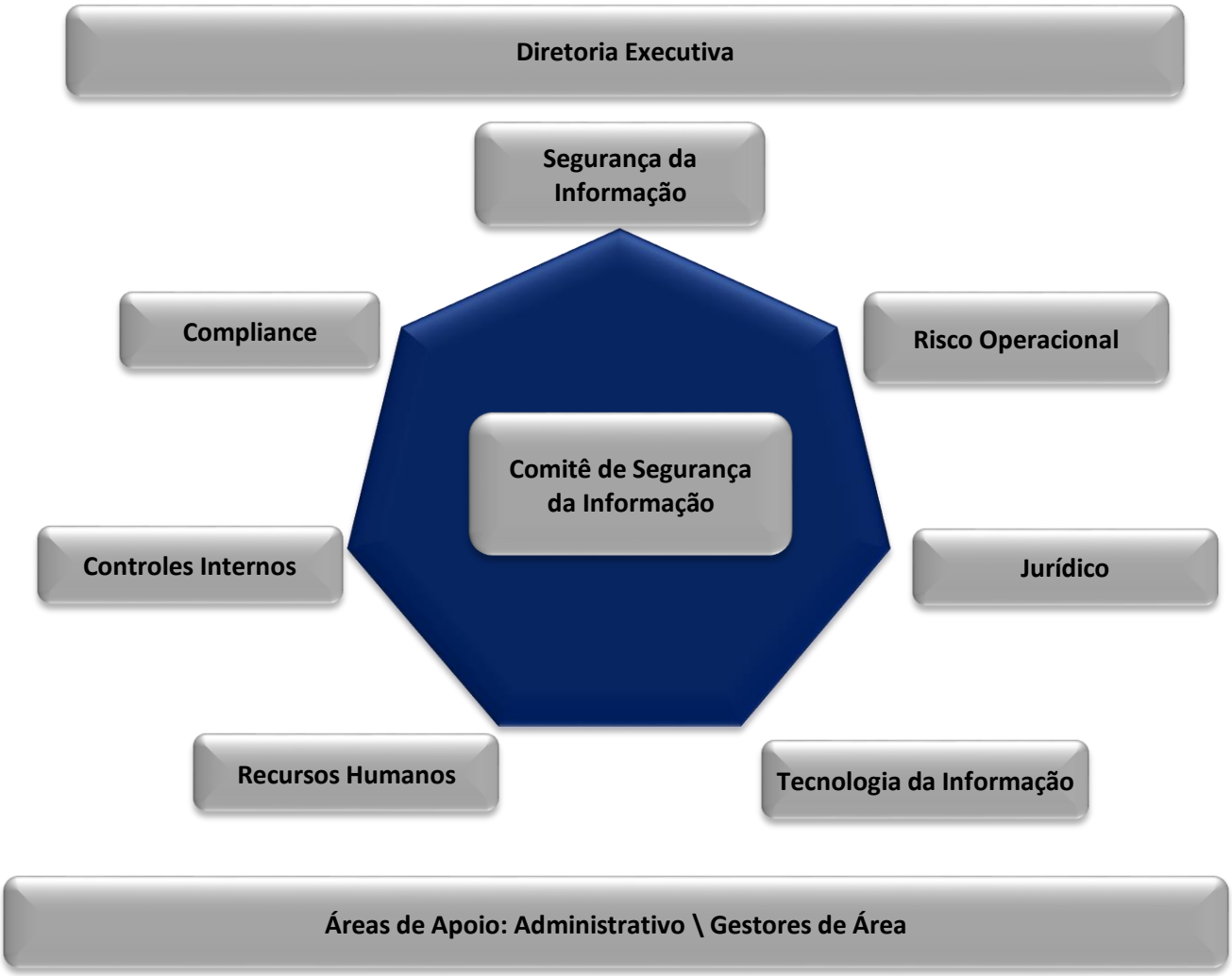
5.4. Manuais e Recomendações:

São documentos que descrevem, por exemplo. Padrões de instalação e configuração segura para determinadas plataformas.

6. ORGANIZACÃO ESTRUTURAL E COMPOSIÇÃO DO COMITÊ

No Grupo Brasil Plural, são adotados modelos de estrutura descentralizada a fim de assegurar isenção ou potenciais conflitos de interesses.

Como forma de ilustrar o acima exposto, a seguir, pode ser observada a organização estrutural e a composição do Comitê, no tocante à Segurança das Informações, Segurança Cibernética, Privacidade no Grupo Brasil Plural, e às áreas de apoio:



7. RESPONSABILIDADE

Em linha com o escopo desta política, seguem abaixo transcritos os papéis e responsabilidades detalhados de cada área.

7.1. Da Diretoria Executiva

Composto por CEO's e Diretores Estatutários do Grupo Brasil Plural é de sua responsabilidade:

- Aprovar as Políticas da organização que tratem sobre Segurança da Informação, Segurança Cibernética e Privacidade.
- Aprovar o relatório anual sobre a implementação do plano de ação e de resposta a incidentes conforme a resolução 4658 do Bacen.

7.2. Do Comitê de Segurança da Informação

O Comitê de Segurança da Informação é formado pelas áreas de Segurança da Informação, Compliance, Risco Operacional, Controles Internos, Jurídico, Recursos Humanos e Tecnologia da Informação.

É de responsabilidade do Comitê de Segurança da Informação:

- Estabelecer, revisar e atualizar as Políticas que tratem sobre Segurança da Informação, Segurança Cibernética e Privacidade anualmente ou quando necessário;
- Aprovar as Normas sobre Segurança da Informação, Segurança Cibernética e Privacidade;
- Debater regularmente sobre leis, normas e regulamentos referentes ao tema;
- Deliberar sobre as decisões e ações relacionadas à segurança da informação e segurança cibernética e privacidade;
- Reunir-se regularmente e/ou sob demanda para efetuar o tratamento dos assuntos relacionados à segurança da informação, segurança cibernética e privacidade, delegando responsabilidades e definindo alçadas de atuação;
- Avaliar os diversos tipos de riscos relacionados à segurança cibernética e deliberar sobre as ações de mitigação apresentadas;
- Analisar e aprovar e acompanhar a execução de planos de ação, estratégias e controles de segurança da informação;
- Submeter para a avaliação do Comitê Disciplinar mencionando o Código de ética e Conduta, casos que descumpram a Política de Segurança da Informação e Política de Segurança Cibernética e Política de Privacidade;
- Analisar os investimentos propostos pela área de Segurança da Informação e submeter à aprovação da Diretoria;
- Assegurar existência de processo estruturado de informação e comunicação de incidentes e violações de segurança;
- Realizar e atualizar o conteúdo do programa de conscientização dos colaboradores do grupo;
- Submeter o relatório anual relativo à Resolução 4658 à aprovação da Diretoria Executiva; e
- Prezar pela confidencialidade das informações de clientes, dentro de sua alçada de atuação.

7.3. Da Área de Segurança da Informação

Tem a atribuição de acompanhar a implantação e manutenção da Política de Segurança da Informação, Política de Segurança Cibernética e Política de Privacidade.

Suas principais atividades são:

- Participar ativamente do Comitê de Segurança da Informação presidindo as reuniões;
- Elaborar pauta, ata e divulgar, em conjunto com o Departamento de Compliance, as deliberações do Comitê de Segurança da Informação;
- Estabelecer e atualizar Normas e Procedimentos que definam a Segurança da Informação e Segurança Cibernética;
- Viabilizar e acompanhar a implantação das Políticas, Normas e os Procedimentos de

  Segurança da Informação, Segurança Cibernética e Privacidade;
- Apoiar e disseminar a cultura de Segurança da Informação; Segurança Cibernética e Privacidade;
- Elaborar e propor medidas, arquiteturas e processos pertinentes à Segurança da Informação; Segurança Cibernética e Privacidade;
- Avaliar e garantir que todos os requisitos para a segurança sejam atendidos, quando da inclusão de novos ativos de TI;
- Assegurar que todos os procedimentos e controles para utilização dos ativos atendem às exigências de integridade, confiabilidade e confidencialidade dos dados e informações, assim como a continuidade das operações dos negócios;
- Zelar pela adequação, efetividade e eficácia das tecnologias de segurança utilizadas

  (hardwares, softwares, técnicas de criptografia, firewalls, autenticadores, antivírus) e

  demais recursos pertinentes;
- Definir e implementar solução que garantam a proteção das informações de acordo com a classificação estabelecida pelas áreas;
- Definir necessidades de investimentos em Segurança da Informação e Segurança Cibernética e submeter à aprovação do Comitê de Segurança da Informação;
- Monitorar o ambiente tecnológico gerenciando as vulnerabilidades e os riscos associados;
- Definir procedimentos e controles adotados para reduzir a vulnerabilidade da instituição;
- Identificar e monitorar os diversos tipos de riscos relacionados à segurança cibernética e apresenta-los para o Comitê de Segurança da Informação para realizar as tratativas de mitigação e controle dos mesmos;
- Assegurar que exista um processo estruturado para registrar e informar os incidentes e violações de segurança em tecnologia da informação;
- Definir controles específicos voltados para a rastreabilidade da informação, que busquem garantir a segurança de informações sensíveis;
- Definir procedimentos e controles para atender leis e regulamentações sobre segurança da informação e segurança cibernética e privacidade;
- Elaborar, e analisar os indicadores de tecnologia para Segurança da Informação, Segurança Cibernética e Privacidade, tomando as ações necessárias para que estes se mantenham dentro dos padrões aceitáveis;

- Estabelecer contato com fóruns e entidades ligados à Segurança da Informação; e
- Manter o Comitê de Segurança da Informação informado sobre novas tendências e ameaças em segurança da informação.

7.4. Do Compliance

- Participar ativamente do Comitê de Segurança da Informação;
- Garantir que as políticas, normas, procedimentos estão em conformidade com as leis e regulamentações;
- Participar ativamente das reuniões do Comitê de Segurança da Informação;
- Compartilhar informações de segurança cibernética com os reguladores e autorreguladores, quando aplicável;
- Compartilhar informações sobre incidentes relevantes com as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil; e
- Diligenciar no sentido de apurar ações de não conformidade com políticas e normas, e denúncias reportadas por colaboradores das demais áreas ou recebidas através do canal de denúncias. Apresentar os casos ao Comitê de Segurança da Informação e inclusive notificar os responsáveis nos casos de comprovada irregularidade.

7.5. Da área de Risco Operacional

- Participar ativamente do Comitê de Segurança da Informação;
- Monitorar os controles de mitigação dos diversos tipos de riscos operacionais relacionados à segurança da informação e segurança cibernética e Privacidade;
- Definir os parâmetros a serem utilizados na avaliação da relevância dos riscos e incidentes de Segurança da Informação, Segurança Cibernética e Privacidade;
- Identificar, registrar, classificar e monitorar continuamente os riscos operacionais aos quais as empresas do grupo estão expostas no sistema destinado a esta finalidade;
- Promover a análise de possíveis deficiências e a exposição de riscos de cada atividade ou processo. Assim como verificar e avaliar os controles mitigadores dos riscos presentes em cada atividade;
- Informar o regulador da contratação de sistemas relevantes dentro do prazo instituído na legislação vigente;
- Elaborar relatórios gerenciais tempestivos para a diretoria versando sobre a aderência dos indicadores de risco de tecnologia aos termos da RAS;
- Elaborar, atualizar e gerenciar o PCN, testes, simulações; e
- Reportar imediatamente ao Compliance a detecção de situações de não conformidade com as Políticas e Normas de Segurança da Informação, Segurança Cibernética e Privacidade.

7.6. Controles Internos

- Participar ativamente do Comitê de Segurança da Informação;
- Avaliar as decisões do Comitê de Segurança da Informação, observando eventuais desvios na eficácia dos controles atualmente executados;

- Revisar periodicamente os procedimentos e controles para concessão de acesso e perfil aos ativos da informação;
- Revisar periodicamente os acessos e perfis concedidos aos ativos da informação;
- Implementar programa de monitoramento periódico, testando e identificando riscos e falhas nas regras e controles estabelecidos, objetivando assegurar a eficácia do sistema de Segurança da Informação, Segurança Cibernética e Privacidade; e
- Cumprir o programa de monitoramento periódico de controles internos, reportando eventuais pontos de atenção identificados ao Comitê de Segurança.

7.7. Da área de Tecnologia da Informação

- Participar ativamente do Comitê de Segurança da Informação;
- Atualizar regras e procedimento técnicos referentes a prevenção e proteção ativos de tecnologia;
- Registrar e analisar a causa e o impacto, bem como controlar os efeitos de incidentes relevantes para as atividades da instituição;
- Manter soluções de prevenção e proteção de dados sempre atualizadas;
- Proteger os dados através de backups periódicos;
- Realizar diligência na contratação de serviços de terceiros, inclusive serviços em nuvem;
- Avaliar questões de segurança durante as fases de pré-projeto e desenvolvimento de novos sistemas, softwares ou aplicações;
- Conduzir o processo de investigação interna e apuração de causas e responsabilidades nos incidentes ou violações de segurança;
- Fornecer suporte aos processos de auditoria e controles internos de TI;
- 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;
- Implementar indicadores definidos pela área de Segurança da Informação, tomando as ações necessárias para que estes se mantenham dentro dos padrões de segurança aceitáveis;
- 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;
- Administrar as soluções tecnológicas de segurança, implementadas pela área de Segurança da Informação, de acordo com as Políticas, Normas e Procedimentos e as melhores práticas de mercado;
- Garantir que as proteções definidas pela área de Segurança da Informação para atender as informações classificadas pelas áreas sejam administradas corretamente;
- Garantir a confidencialidade, disponibilidade e integridade das informações armazenadas nos equipamentos, sistemas e bases de dados do Grupo Brasil Plural;

- 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;
- Elaborar o Plano de Recuperação de Desastres (DRP); e
- Gerenciar processos de mudanças e de retorno à normalidade (na eventualidade de crises, incidentes e emergências que acarretem no acionamento do PCN).

7.8. Do Jurídico

- Definir e consolidar as provas e evidências necessárias para possibilitar a aplicação das penalidades a serem decididas no Comitê Disciplinar, 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 as 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 disponham sobre acordos de SLA (Acordo de Nível de Serviço), responsabilidades e que visem preservar a segurança das informações do Grupo Brasil Plural e, principalmente, de seus clientes;
- 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 pela Genial Investimentos;
- Armazenar os termos de confidencialidade e responsabilidade de todos os fornecedores, prestadores de serviço e parceiros comerciais do Grupo Brasil Plural, alterando, quando necessário, acordos e contratos;
- Controlar a vigência de contratos celebrados; e
- Monitorar para que as rescisões ou alterações em contratos não exponham o Grupo Brasil Plural a impactos negativos (de qualquer ordem) relacionados à Segurança da Informação. Uma das medidas é sempre inserir cláusulas de confidencialidade em todos os contratos firmados pelas empresas do Grupo Brasil Plural.

7.9. Área de Gente

- 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 Grupo Brasil Plural;
- Checar informações pessoais e profissionais prestadas pelos Colaboradores no processo de contratação;
- Organizar e coordenar a realização de treinamentos internos sobre Segurança das Informações;
- Aplicar, as penalidades para as violações e incidentes de Segurança da Informação, de acordo com a decisão do Comitê Disciplinar;
- Em caso de observar, em entrevistas de desligamento, indícios de mau uso ou vazamento de informações (ou possibilidade), comunicar o fato imediatamente ao Comitê de Segurança da Informação; e

7.10. Departamento Pessoal

- Garantir que os novos Colaboradores tenham acesso as Políticas de Segurança da Informação, Política de Segurança Cibernética e Política de Privacidade, disponibilizando o Manual de Segurança da Informação para os Colaboradores;

- Garantir que os termos de Confidencialidade e de Responsabilidade sejam assinados pelo Colaboradores;
- Armazenar os termos de confidencialidade e responsabilidade de todos os Colaboradores (inclusive temporários), alterando, quando necessário, a descrição de cargos;
- Comunicar imediatamente, via sistema de Service Desk, informações sobre movimentações de Colaboradores (transferências, promoções, demissões, desligamentos, licenças, férias, suspensões ou admissões) para que as concessões e revogações de acesso sejam realizadas corretamente;
- 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.

7.11. Administrativo

- Classificar os meios de informação não computadorizados que administra quanto à relevância para o Grupo 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 administrativos 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;
- Coordenar a recepção de clientes e visitantes, garantindo que não circulem nas dependências desacompanhados evitando assim o acesso a áreas seguras da empresa;
- Gerenciar os serviços de expedição de documentos e correspondências garantindo assim a confidencialidade e integridade das mesmas;
- 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 que contenha informações de propriedade do Grupo Brasil Plural;
- Gerenciar os procedimentos inerentes à identificação e ao acesso físico de Colaboradores, clientes e visitantes do Grupo Brasil Plural;
- Administrar os serviços de segurança patrimonial (proteção, monitoramento 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.

7.12. Diretoria

- Disseminar a importância do cumprimento de todo o conteúdo disposto nas Políticas, Normas e Procedimentos referentes a Segurança da Informação, Segurança Cibernética e Privacidade a toda organização;
- Avaliar e deliberar sobre os investimentos propostos pela área de Segurança da Informação analisados e aprovados pelo Comitê de Segurança da Informação;

- Definir a correta classificação das informações sob sua responsabilidade de acordo com a sua importância para a organização; e
- Garantir que os dados e informações sob sua responsabilidade receba a correta proteção no ciclo de vida da informação, garantindo assim a sua confidencialidade, integridade e disponibilidade cumprindo as leis e regulamentações vigentes.

7.13. Dos Gestores das Áreas

- Disseminar aos colaboradores sob sua gestão, a política, normas, procedimentos e padrões que eles deverão seguir e respeitar;
- Identificar e classificar arquivos, documentos e recursos relevantes sob sua responsabilidade;
- Comunicar, previamente a área de Recursos Humanos, situações referentes à movimentação de pessoal (transferências, promoções, demissões, desligamentos, licenças, férias, suspensões ou admissões);
- Solicitar a área de Service Desk o bloqueio imediato dos acessos de colaboradores que tenham acesso a informações sensíveis e confidenciais quando o mesmo for ser desligado;
- Reportar imediatamente aos canais de denúncias, a área de Compliance ou a equipe de Segurança da Informação quaisquer suspeitas de não conformidades ou violação com as regulamentações e definições constantes da Políticas, Normas ou Procedimentos referentes a Segurança da Informação Segurança Cibernética ou Privacidade;
- Prover planos de continuidade e contingência que garantam, as condições mínimas necessárias de atuação da sua área em uma situação de anormalidade;
- Responsabilizar-se pela propriedade das informações de sua área ou quando a classificação da informação assim exigir; e
- Manter-se sempre ativo e aplicado sobre as demais responsabilidades de sua gestão que constam nas Políticas de Segurança da Informação, Política de Segurança Cibernética e Política de Privacidade do Grupo Brasil Plural.

7.14. Dos Demais Colaboradores

- Respeitar e cumprir todo o conteúdo disposto nas Políticas, Normas e Procedimentos do Grupo Brasil Plural;
- Ter ciência de que todas as informações geradas, acessadas, processadas, utilizadas ou armazenadas em qualquer meio ou sistema de informação que utilizem no exercício de sua função, são de propriedade do Grupo Brasil Plural e devem ser relacionadas às suas atividades profissionais e poderão ser monitoradas ou auditadas;
- Reportar para a equipe de Service Desk qualquer incidente ou ação de anormalidade;
- Reportar imediatamente aos canais de denúncias, a área de Compliance ou a equipe de Segurança da Informação quaisquer suspeitas de não conformidades ou violação com as regulamentações e definições constantes da Políticas, Normas ou Procedimentos referentes a Segurança da Informação Segurança Cibernética ou Privacidade; e
- Participar dos treinamentos e disseminar a cultura e importância de todos agirem com responsabilidade no tratamento das informações.

7.15. Dos Prestadores de Serviços

- Respeitar e cumprir todo o conteúdo disposto nas Políticas, Normas e Procedimentos do Grupo Brasil Plural; e
- Registrar e analisar a causa e o impacto, bem como controlar os efeitos de incidentes de segurança relevantes.

Violação da Política de Segurança Cibernética

O descumprimento de alguma regra constante nesta política será considerado como falta Grave, conforme disposto nos Código de Ética e Conduta do conglomerado Brasil Plural ou de acordo com análise de decisão de Comitê de Segurança da Informação, sujeitando o Colaborador à sanções administrativas de acordo com o grau de severidade do incidente.

genialinvestimentos.com.br