# Política de Segurança Cibernética

## Abril de 2019

**Elaboração:** Comitê de Segurança da Informação

**Aprovação:** Diretoria Executiva

**Classificação:** Público

## 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 n° 4.658 do Banco Central do Brasil, de 26 de abril de 2018, observando a natureza das suas operações, a complexidade dos produtos, serviços, atividades e processos, bem como o 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. Conceito

A Segurança Cibernética, constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

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

i. Confidencialidade: Garantir que as informações sejam acessadas apenas por pessoas autorizadas;

ii. Integridade: Garantir que as informações, tanto em sistemas quanto em bancos de dados, estejam em um formato verdadeiro e correto para seus propósitos originais;

iii. Disponibilidade: Garantir que as informações e os recursos estejam disponíveis para aqueles que precisam deles quando necessário;

iv. 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;

v. Incidente de Segurança da Informação: Um incidente de segurança da informação pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança, que pode comprometer a Confiabilidade, Integridade e/ou Indisponibilidade da informação.

## 3. Abrangência

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

- PLURAL S.A. BANCO MULTIPLO
- GENIAL INSTITUCIONAL CORRETORA DE CAMBIO, TITULOS E VALORES MOBILIARIOS S.A
- GENIAL INVESTIMENTOS CORRETORA DE VALORES MOBILIARIOS S.A

## 4. Estrutura Organizacional

No Grupo Plural, são adotados modelos de estrutura descentralizada a fim de assegurar isenção ou potenciais conflitos de interesses. A organização estrutural e sua composição no que tange à segurança cibernética estão disponíveis nas Políticas de Segurança da Informação do Grupo.

## 5. Responsabilidade

Em linha com o escopo desta política, seguem abaixo transcritas os papéis e responsabilidades detalhados e segmentados.

### 5.1. Do Comitê de Segurança da Informação

- Revisar e atualizar esta Política anualmente ou quando necessário, em conjunto com as demais áreas integrantes do Comitê de Segurança da Informação;
- Deliberar sobre as decisões e ações relacionadas à segurança cibernética;
- Monitorar ativamente e tratar dos assuntos referentes ao tema em nível estratégico, tático e operacional;
- Conduzir o processo de investigação interna e apuração de causas e responsabilidades nos incidentes ou violações de segurança;
- Reunir-se para efetuar o tratamento dos assuntos relacionados à segurança cibernética, delegando responsabilidades e definindo alçadas de atuação;
- Submeter para a avaliação do Comitê Disciplinar mencionando o Código de ética e Conduta, recomendações de penalidades e ações a serem tomadas para os casos não previsto nesta Política;
- Monitorar ativamente a observância dos dispositivos contidos nesta Política;
- Definir de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição;
- Deliberar sobre a classificação dos dados e das informações quanto à relevância;

- Manter-se sempre ativo e aplicado sobre as demais responsabilidades de sua gestão que constam nas Políticas de Segurança da Informação do Grupo Plural.

## 5.2. Da Área de Tecnologia da Informação

- Definir procedimentos e controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética e publicá-los em documento interno específico para seu registro;
- Definir controles específicos voltados para a rastreabilidade da informação, que busquem garantir a segurança de informações sensíveis e publicá-los em documento interno específico para seu registro;
- 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 e publicá-los em documento interno específico para seu registro;
- Definir os parâmetros a serem utilizados na avaliação da relevância dos incidentes e publicá-los em documento interno específico para seu registro;
- Compartilhar informações sobre incidentes relevantes com as demais instituições;
- 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;
- Manter-se sempre ativo e aplicado sobre as demais responsabilidades de sua gestão que constam nas Políticas de Segurança da Informação do Grupo Plural.

## 5.3. Do Compliance

- Ministrar treinamento referente ao conteúdo desta política, sempre que necessário;
- Manter-se sempre ativo e aplicado sobre as demais responsabilidades de sua gestão que constam nas Políticas de Segurança da Informação do Grupo Plural.

## 5.4. Da Unidade de Gerenciamento de Riscos

- Identificar, avaliar, monitorar, controlar e mitigar os diversos tipos de riscos operacionais relacionados à segurança cibernética;
- Classificar os dados e informações quanto à relevância;
- Definir os parâmetros a serem utilizados na avaliação da relevância dos incidentes;
- Registrar os riscos operacionais no sistema de controle;
- Elaborar relatórios gerenciais tempestivos para a diretoria versando sobre a aderência dos indicadores de risco de tecnologia aos termos da RAS;
- Manter-se sempre ativo e aplicado sobre as demais responsabilidades de sua gestão que constam nas Políticas de Segurança da Informação do Grupo Plural;
- Elaborar cenários de incidentes considerados nos testes de continuidade de negócios;

## 5.5. Da Área de Auditoria Interna

- Verificar o cumprimento desta política e dos procedimentos. Realizar anualmente testes de avaliação com o objetivo de verificar a aderência aos fundamentos estabelecidos nesta política.

## 5.6. Dos Gestores das Áreas

- Disseminar aos colaboradores sob sua gestão, a política, controles, procedimentos e padrões que eles deverão seguir e respeitar;
- Responsabilizar-se pela propriedade das informações de sua área ou quando a classificação da informação assim exigir;
- Manter-se sempre ativo e aplicado sobre as demais responsabilidades de sua gestão que constam nas Políticas de Segurança da Informação do Grupo Plural.

## 5.7. Da Alta Administração

- Buscar a melhoria contínua dos procedimentos relacionados com a segurança cibernética;

## 5.8. Dos Demais Colaboradores

- Respeitar e cumprir todo o conteúdo disposto nesta política e nas demais políticas do Grupo;
- 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 ou auditadas.
- Reportar para as áreas responsáveis qualquer violação ou incidente de segurança da informação;
- Participar dos treinamentos e disseminar a cultura e importância de todos agirem com responsabilidade no tratamento das informações;
- Prestar informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros;

- Manter-se sempre ativo e aplicado sobre as demais responsabilidades de sua gestão que constam nas Políticas de Segurança da Informação do Grupo Plural.

### 5.9. Dos Prestadores de Serviços

- Registrar e analisar a causa e o impacto, bem como controlar os efeitos de incidentes de segurança relevantes.

## 6. Diretrizes

Para assegurar que as informações confidenciais sejam adequadamente protegidas, as instituições que fazem parte do conglomerado Plural definiram os seguintes processos e controles:

### 6.1. Controle de segurança cibernética

Os controles de segurança cibernética, devem estar alinhados e acordados entre a estrutura da organização, porém a sua execução deverá ser garantida pela área de Tecnologia da Informação:

- Proteção de dados armazenados, com ferramenta segura de backup e criptografia, conforme a necessidade;
- Bancos de dados e dispositivos de rede com segurança dedicada que seja rigorosamente controlado para preservar a integridade, a confidencialidade e a disponibilidade do conteúdo;
- Manutenção e atualização dos sistemas operacionais e softwares utilizados na instituição;
- Prevenção de ameaças com firewalls, antivírus, perfis de acesso específico para os administradores dos sistemas/redes, filtros de spam, controle para uso de periféricos, soluções de prevenção e correções de vulnerabilidades e filtros de uso de internet;
- Inclusão das preocupações de segurança durante as fases de desenvolvimento de novos sistemas, softwares ou aplicações;
- Controles de auditoria, tais como sistemas de gerenciamento de senhas, logs e trilhas de acesso;
- Contrato de manutenção com Suporte 24x7 dos servidores e rede.

### 6.2. Testes de controles

A efetividade da política de segurança cibernética deve ser verificada por meio de testes e revisões periódicas dos controles existentes. O plano de teste deve ser executado pela área de Tecnologia da Informação assegurando que:

- Os acessos dos colaboradores estão em conformidade com os acessos as áreas de atuação,
- Que os níveis de confidencialidade e acessos as informações confidenciais estão adequadas;
- Recursos computacionais de controle de acesso físico e lógico, estejam protegidos;
- Que haja rastreabilidade de registros que permitam a realização de auditorias periódicas.

## 7. Incidente de Segurança da Informação

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

- 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;
- Incidentes comportamental deverá ser reportado para a área de Compliance ou à para algum membro do Comitê de Segurança da Informação, que analisará caso a caso e adotará as medidas cabíveis conforme estabelecido na Política de Segurança da Informação.

## 8. Treinamento

Todos os colaboradores das Instituições do Grupo Plural, deverão aderir à política, receber periodicamente treinamentos e materiais educativos que visem a conscientização e/ou reciclagem de conhecimento sobre o tema.

## 9. Penalidades

O descumprimento de alguma regra desta política será considerado como falta Grave, conforme disposto nos Código de Ética e Conduta do Grupo Plural ou de acordo com análise de decisão de Comitê, sujeitando o Colaborador a sanções administrativas de acordo com o grau de severidade do incidente.

## 10. Documentos relacionados

Esta política foi elaborada com base nos controles e documentações internas relacionados as diretrizes e tratamento da segurança da informação do Grupo Plural. São elas:

- Manual de Segurança da Informação - Plural
- Política de Segurança da Informação - Genial Investimentos
- Política de Gerenciamento de Risco Operacional
- Plano de Continuidade de Negócios
- Código de Ética e Conduta