Sumário

1 INTRODUÇÃO

A informação pode existir em várias formas. Qualquer forma que ela tenha ou os meios em que seja compartilhada ou armazenada sempre precisa ser protegida. A continuidade do nosso negócio está diretamente ligada à disponibilidade e confiabilidade dos nossos sistemas de informação

Sistemas de informação, sendo vetores de comunicação, são essenciais para nossas atividades, e representam uma grande vantagem competitiva. De fato, a informação manipulada por estes sistemas é um ativo que, assim como outros ativos importantes da empresa, é crucial para as atividades e negócios da Ativos.

2 OBJETIVO

Esta política foi elaborada para estabelecer as estratégias de Segurança da Informação na Ativos. Ela define os papéis e responsabilidades de todos os colaboradores que interagem com a informações e sistemas através do seguinte ciclo de vida: criação, operação, uso e descarte.

Definir as diretrizes que nortearão as normas e padrões que tratam da proteção da informação, abrangendo sua geração, utilização, armazenamento, distribuição, confidencialidade, disponibilidade e integridade, independentemente do meio em que ela esteja contida.

3 PREMISSAS

Esta política declara a necessidade de uma governança de Segurança da Informação eficiente. Esta governança é baseada em:

a. **Comitê Gestor de Segurança da Informação (CGSI)**: assegurar que as estratégias de segurança da informação estejam alinhadas com as estratégias de negócios e os níveis de risco associados com os sistemas de informação sejam aceitáveis para a Ativos.

b. **Departamento de Segurança da Informação:** realizar a governança de segurança da informação e provisão de soluções, serviços e gestão de identidade e acessos ao ambiente lógico pertinente a Ativos.

c. **Gestor de Segurança da Informação:** tem como principal responsabilidade a implementação de estratégias de segurança, levando em conta as particularidades da Ativos a qual ele é responsável.

Mantidos sob controle da Ativos, os riscos de negócios associados com os sistemas de informação requerem uma estratégia bem definida e um comprometimento da Alta Gestão nesta estratégia, tais como: alocação de recursos necessários, a implementação de medidas efetivas, melhores práticas de segurança da informação e construção de um ambiente de negócio seguro.

Avaliações são conduzidas regularmente nas unidades de negócio e departamentos da Ativos. As recomendações resultantes dessas avaliações são revisadas e compartilhadas. É de responsabilidade das unidades de negócio e departamentos a implementação de um plano de ação para reduzir os riscos identificados a um nível aceitável.

Esta política também especifica as regras de segurança a serem seguidas nas seguintes áreas:

Conscientização de Segurança da Informação

Os colaboradores, usuários, prestadores de serviço, terceiros devem estar conscientes dos fatores essenciais sobre o assunto segurança da informação, incluindo o porquê de os controles de segurança serem necessários. Eles precisam entender as responsabilidades pessoais no contexto de segurança para assegurar que os controles sejam implementados devidamente e para prevenir o compartilhamento ou divulgação de informações sensíveis para pessoas não autorizadas.

Segurança em Contratos de Prestação de Serviços (Terceiros)

Contratos com terceiros (prestadores de serviços) envolvendo acesso, processamento, comunicação ou manipulação de informações da Ativos ou processamento de informações em locais remotos precisam conter todas as cláusulas de segurança da informação relevantes e Acordo de Confidencialidade ou (NDA – Non Disclosure Agreement).

Proteção de Informação

As informações armazenadas ou processadas por aplicações de negócios ou serviços de TI devem ser protegidas de acordo com seu nível de criticidade para os negócios.

Gestão de Acesso Físico e Lógico

Mecanismos efetivos de controle de acesso reduzem o risco de acesso não autorizado às informações e sistemas. Desta forma, essa área contempla a disciplina de controle de acessos aplicados a usuários e as medidas a serem tomadas para restringir acesso à informação dentro dos sistemas da Ativos e manter os acessos apropriados em uma perspectiva de longo prazo.

Segurança de Aplicações de Negócio

Aplicações críticas de negócios necessitam controles de segurança mais incisivos do que as outras aplicações. Entendendo o impacto que pode ser causado nos negócios por causa

de uma perda de confidencialidade, integridade ou disponibilidade de informação, é possível estabelecer o nível de importância de uma aplicação. Isso provê uma base sólida para identificar riscos à informação e determinação de níveis de proteção requeridos para manter uma informação num nível de risco aceitável.

Continuidade dos Negócios

No caso de um evento extraordinário, os sistemas podem ficar indisponíveis por um longo período. Uma solução de contorno é necessária para possibilitar a organização a continuar as operações e reduzir os impactos ao mínimo aceitável. As regras nesta área incluem o desenvolvimento de planos e procedimentos de emergência e as respectivas validações.

Segurança de Equipamentos de TI

Os colaboradores têm maior probabilidade de executar adequadamente suas atividades se os equipamentos de TI forem dimensionados corretamente. Assim, essa área de conhecimento cobre o planejamento de equipamentos de TI e ambientes, calculando eventos relacionados à segurança e a configuração de servidores e estações de trabalho.

Segurança de Redes

Redes de computadores transmitem informações e provém um canal de acesso aos sistemas de informação. Por natureza, elas são bastante vulneráveis a interrupções dos serviços e ataques. Manter a comunicação da área de negócio segura, requer uma rede bem planejada, serviços de redes bem definidos e monitoramento de segurança das redes. Esses fatores se aplicam igualmente tanto a redes locais, redes remotas, sobre comunicações de dados e voz.

Encriptação e Hashing

Para garantir a confidencialidade dos dados em trânsito e repouso, faz-se necessário a aplicação de protocolos de encriptação e/ou hashing, dependendo de fatores como escopo, tecnologia, complexidade, compatibilidades. Dados que não possuem encriptação ou hashing estão suscetíveis à acesso, leitura e compartilhamento não autorizados. Essa área de conhecimento cobre o assunto supracitado, estabelecendo inclusive premissas para implementação.

4 ABRANGÊNCIA

Aplicam-se a todos os colaboradores da e/ou prestadores de serviços terceirizados, assim como parceiros, fornecedores, clientes e todas as pessoas que, de alguma forma, tenham acesso às informações da Ativos em qualquer meio ou suporte que ela se encontre (ex.: papel, mídias diversas, comunicação verbal, entre outros).

5 REFERÊNCIAS

As regras de segurança da informação detalhadas nesta política estão de acordo com as melhores práticas de segurança, referenciada nos padrões da ISO 27002. De qualquer maneira, a relevância de cada regra é determinada de acordo com os riscos específicos da Ativos e sua implementação deve ser revisada regularmente.

6 DEFINIÇÕES

6.1 O que é Segurança da Informação (SI)?

Segurança da informação é a proteção da informação contra vários tipos de ameaças, visando garantir a continuidade do negócio, minimizando riscos e maximizando o retorno sobre os investimentos e as oportunidades para a organização.

Quando não gerenciados adequadamente, os riscos e ameaças relativos à informação podem causar consideráveis danos e prejudicar o crescimento e vantagem competitiva.

Segurança da Informação são esforços contínuos para a proteção de ativos de informação, para tanto visa atingir os seguintes objetivos:

Disponibilidade: a Política de Segurança da Informação deve ser divulgada a todos os colaboradores da Ativos e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento;

Integridade: a informação deve estar correta, ser verdadeira e não estar corrompida;

Confidencialidade: a informação deve ser acessada e utilizada exclusivamente pelos que necessitam dela para a realização de suas atividades profissionais na Ativos; para tanto, deve existir autorização prévia;

Autenticidade: a informação deve conferir certeza sobre sua identidade inequívoca em qualquer sistema pelo qual ela se comunique, bem como deve ser apta a validar a identificação plena de tais meios;

Irretratabilidade: a informação deve ser capaz de conferir a autoria inequívoca do responsável por sua criação, alteração, transmissão e até mesmo eliminação, de forma a garantir o não repúdio.

A segurança é obtida a partir de adoção de um conjunto de melhores práticas de mercado, incluindo políticas, procedimentos, estruturas organizacionais e funções de softwares e hardwares.

É fundamental para proteção e salvaguarda das informações que os usuários adotem a ação de Comportamento Seguro (leia-se Política de Uso da Informação) e consiste com o objetivo

de proteção das informações, devendo assumir atitudes proativas e engajadas no que diz respeito à proteção das informações.

6.2 Por que a Segurança da Informação é necessária?

A informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Definir, alcançar, manter e melhorar a segurança da informação são atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da Ativos junto ao mercado.

Atualmente, as empresas estão expostas a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Danos causados por código malicioso, hackers e ataques de negação de serviço estão se tornando frequentes e incrivelmente sofisticados.

A Política de Segurança da Informação deve ser considerada uma diretriz de alto nível e seu cumprimento exige a implementação de controles e processos em todas as Unidades de Negócio da Ativos.

Orientar os procedimentos básicos de manuseio, armazenamento, transporte e descarte da informação como recurso estratégico aos negócios.

7 PAPÉIS E RESPONSABILIDADES

7.1 Governança de Segurança

7.1.1 Princípios de Governança

A governança de segurança da Informação da Ativos conduz iniciativas de segurança baseada nos seguintes princípios (conhecidos como os 5 pilares da governança em segurança da informação):

I. **Alinhamento estratégico:** do setor de Segurança da Informação com estratégias de negócio para atender às demandas e objetivos do negócio;

II. **Gerenciamento de riscos:** através da execução de medidas apropriadas para administrar, mitigar riscos e reduzir potenciais impactos nos ativos da organização para um nível aceitável;

III. **Gerenciamento de recursos:** usados o conhecimento de segurança da informação e infraestrutura de maneira eficiente e eficaz;

IV. **Mensuração de performance:** medindo, monitorando, e mostrando métricas de governança da informação robustas e auditáveis, para se assegurar que os objetivos sejam atingidos;

Valor de entrega otimizando investimentos em segurança da informação para suportar os objetivos da Ativos.

7.1.2 Responsabilidades de Segurança da Informação

Cabe a todos os colaboradores (colaboradores, estagiários e prestadores de serviços) cumprir fielmente a Política de Segurança da Informação; buscar orientação do 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 a sua disposição sejam utilizados apenas para as finalidades aprovadas pela Ativos; 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, através do canal de ética, etica@rodobens.com.br.

7.2 Gestor da Informação

O gestor da informação deve ser indicado pela direção geral da organização, é o executivo da área responsável por processos e sistema de informação. Este gestor é a pessoa responsável pelo segurança da informação referente a sua Unidade de Negócio.

O gestor deve indicar uma segunda pessoa para também exercer esta função, como medida de contingência. Suas principais atribuições são:

I. Identificar e classificar periodicamente as informações relativas à sua área de atuação, quanto ao seu grau de importância e sigilosidade assim como estabelecer regras de proteção que devem ser conferidas às mesmas;
II. Autorizar o acesso de outros colaboradores às informações sob sua responsabilidade;
III. Definir a periodicidade de realização e o prazo de retenção das cópias de segurança das informações fundamentais à continuidade dos negócios da Ativos que estejam sob sua gestão;
IV. Auxiliar na elaboração do plano de contingência e acompanhar os testes periódicos de validação do plano;
V. Autorizar formalmente as modificações a serem efetuadas nos sistemas e processos que envolvam as informações de sua área.

7.3 Tecnologia da Informação

É a área responsável pela gestão dos ativos de processamento e disponibilidade de ambientes de informação. Tem a responsabilidade de:

I. Implantar e administrar as regras de proteção definidas pelo Comitê Gestor de Segurança da Informação - CGSI, revisando-as periodicamente, em conjunto com ele;
II. Orientar tecnicamente os demais colaboradores sobre aspectos relacionados à Segurança da Informação;
III. Participar na elaboração e efetivação do plano de contingência;
IV. Detectar, identificar e comunicar à área de Segurança da Informação, as tentativas ou violações de acesso não autorizado;
V. Executar e manter cópias de segurança (backup) de toda informação fundamental aos negócios da Ativos.

7.4 Líder/Gestor/Executivo

É toda pessoa detentora de função de liderança e que define o tipo de acesso a ser concedido aos colaboradores sob sua supervisão. Suas responsabilidades são:

- Comunicar a TI - Segurança da Informação e ao gestor de sistema toda e qualquer movimentação ou alteração de perfil funcional do colaborador sob sua responsabilidade, que implique: alteração, inclusão, suspensão ou cancelamento de acesso concedido (vide Política de Gestão de Acessos a Redes e Sistemas);

- Zelar pela proteção das informações, verificando o cumprimento das diretrizes e disseminando as boas práticas de Segurança da Informação entre toda sua equipe;

- Garantir que todo colaborador sob sua supervisão tenha acesso às diretrizes de segurança da informação, ao Código de Ética e tenha assinado o termo de responsabilidade de uso de recursos tecnológicos.

7.5 Usuário da Informação

São todos os colaboradores e/ou prestadores de serviços terceirizados, assim como parceiros, fornecedores, clientes e todas as pessoas que, de alguma forma, tenham acesso à informação para desempenho de suas atribuições funcionais, em conformidade com os perfis de acesso definidos pelo gestor da informação. Suas responsabilidades são:

- Tomar ciência da Política de Segurança da Informação e cumprir suas normas e procedimentos;

- Elucidar com seu líder ou responsáveis por Segurança da Informação, qualquer dúvida sobre condutas e procedimentos a serem seguidos com relação às informações a que tem acesso;

- Usar a informação e todos os recursos a ela relacionados somente para os fins estabelecidos pelo gestor;

- Manter sigilo sobre suas senhas de acesso aos sistemas e informações da Ativos;

- Responder por todo e qualquer acesso, bem como pelos efeitos dos acessos realizados com o uso do seu código de identificação e senha (Anexo I);

- Utilizar os canais adequados para encaminhamento ao seu líder ou gestor imediato ou ao comitê gestor da segurança da informação das denúncias de violações da política ou situações de riscos de segurança da informação.

7.6 Gestor de Segurança da Informação

É o responsável pelo planejamento, avaliação e definição de controles de proteção dos ativos de informação da Ativos. O Gestor da Segurança da Informação é a pessoa do Corporativo voltada para normatização da Segurança da informação. Suas responsabilidades são:

- Organizar o escritório de segurança e a infraestrutura organizacional responsável pelo tratamento da segurança (comitês e supervisões de segurança dentre outros) ;
- Planejar os investimentos para a Segurança da Informação;
- Definir indicadores para acompanhamento da gestão de risco e retorno do investimento;
- Orientar e coordenar a equipe e consultorias terceirizadas;
- Gerir a gestão de riscos de tecnologia e operacionais relacionados à segurança da informação;
- Gerir as políticas e procedimentos de Tecnologia e Segurança da Informação;
- Definir, elaborar, divulgar, treinar, implementar e administrar juntamente com sua equipe:

I. Plano estratégico de Segurança;
II. Política de Segurança;
III. Análise de risco e Relatórios de avaliação do nível de segurança;
IV. Plano de auditoria de segurança;
V. Conformidade e atendimento a legislação vigente;
VI. Investigações sobre incidentes de segurança;
VII. Projetos de Segurança, dentre outros.

a) Sugerir e orientar para que a segurança seja parte do processo de planejamento dos negócios;
b) Propor, desenvolver e aprovar políticas, normas e procedimentos de segurança;
c) Discutir, propor e aprovar medidas e eventuais investimentos para melhoria de segurança;
d) Apoiar e promover iniciativas de segurança da informação, como programas de conscientização e outras, bem como, aprovar iniciativas para aumentar o nível da segurança da informação;
e) Avaliar os controles existentes e determinar medidas corretivas caso identifique a necessidade;

f) Determinar revisões periódicas de segurança quando entender necessário.
g) Disponibilizar os canais de comunicação adequados para o recebimento de informações de ocorrências de violações desta política ou situações de riscos de segurança da informação.

7.7 Auditor Interno

É designado pela Ativos para coordenar a revisão de conformidade das operações, produtos e serviços com as diretrizes e padrões estabelecidos, bem como com legislação, regulamentos e contratos vigentes. Suas responsabilidades são:

a) Participar da definição e homologação das diretrizes de Segurança da Informação;
b) Verificar a conformidade das operações, produtos e serviços disponibilizados pela Ativos em relação às diretrizes e padrões de segurança da informação.

Apontar violação de regulamentos ou obrigações contratuais e de quaisquer requisitos de segurança.

7.8 Auditor Externo

Não tem vínculo com a empresa auditada e é designado por um órgão normativo (Banco Central, Susep, CVM) para auditar a conformidade das operações, produtos e serviços com as diretrizes e padrões estabelecidos em legislação e regulamentos destes Órgãos.

7.9 Gente & Gestão

I. Garantir que todo colaborador receba treinamento específico em sua área de atuação;
II. Manter sob sua custódia os Termos de Responsabilidade, Confidencialidade e Sigilo assinados por colaboradores da Ativos;
III. Disseminar e controlar treinamentos aos colaboradores;
IV. Aplicar sanções cabíveis em conjunto com o gestor da unidade de negócio ou departamento, caso necessário.

7.10 Comunicação Interna

I. Apoiar no desenvolvimento de materiais audiovisuais para programas de treinamentos de segurança da informação;
II. Comunicação de conteúdos pertinentes à Segurança da Informação por toda a organização;
III. Divulgação de temática de segurança da informação nos canais oficiais de comunicação (Portal Integra, E-mail etc.).

7.11 Comitê Gestor de Segurança da Informação - CGSI

É o Comitê responsável pela definição das diretrizes de proteção dos ativos de informação. As reuniões ocorrem quando surgem temas que demandam discussões; e tem como objetivo:

- Propor, desenvolver e aprovar a Política de Segurança de Informação;
- Determinar revisões periódicas de Segurança da Informação quando entender necessário;
- Atuar nas decisões de solução das ocorrências referente à segurança da Informação;
- Avaliar riscos a fim de proteger a continuidade dos Negócios da Ativos; propondo medidas e eventuais investimentos para a melhoria da Segurança da Informação.

É composto por representantes das Seguintes Áreas:

i. Corporativo;
ii. Auditoria;
iii. Jurídico;
iv. Diretoria CSC; Compliance;
v. Tecnologia da Informação

7.12 Comitê de Proteção de Dados

Os membros do comitê, empossados de acordo com o Termo de posse dos membros do Comitê de Proteção de Dados são responsáveis por exercerem os papeis atribuídos aos mesmos em cumprimento ao Programa de Privacidade e **Proteção de Dados** e ao Regulamento do Comitê de proteção de dados para cumprimento da Lei Geral de Proteção de Dados.

8 Condições Normativas

8.1 Ativos de Informação

A informação é um recurso vital e estratégico para os negócios da Ativos e como tal deve ser preservada com o nível de segurança proporcional ao impacto decorrente da sua alteração, destruição ou veiculação não autorizada, sejam elas, acidentais ou intencionais.

Devem ser adotados procedimentos preventivos, recursos de segurança e contingência, a fim de minimizar interrupções. Garantir a pronta restauração de sistemas e dados no caso de ocorrência de sinistros ou imprevistos que possam causar indisponibilidade momentânea ou definitiva das informações.

É indispensável que se faça cópia de segurança (backup) de toda informação fundamental aos negócios da Ativos, com retenção equivalente ao impacto que a sua perda, dano ou indisponibilidade causariam ao negócio.

Todas as ações destinadas à proteção da informação devem considerar os aspectos físicos, lógicos e humanos e se estenderem a todos os meios de informação e comunicação sejam eles automatizados ou não.

8.2 Impacto nos Negócios e Análise Financeira em Segurança da Informação

As regras e procedimentos de segurança da Ativos não devem representar obstáculos para a flexibilidade e agilidade dos negócios. Em contrapartida, estas devem ser alcançadas dentro dos limites estabelecidos pela Política de Segurança da Informação.

O impacto causado por uma divulgação não autorizada de informações de negócios e a alteração acidental ou manipulação deliberada da informação armazenada ou processada pelas aplicações de negócio devem ser analisados previamente.

Os investimentos em recursos de tecnologia para a segurança da informação devem buscar sempre a melhor relação custo-benefício, privilegiando as áreas mais críticas e de maior risco para os negócios, observando em especial tecnologias modernas e já de comprovado reconhecimento mercadológico.

Periodicamente será efetuada análise dos riscos associados aos ativos da informação da Ativos, visando avaliar o impacto decorrente de perda, divulgação indevida, destruição e adulteração da informação.

8.3 Análise de Riscos à Segurança da Informação e Controles Internos

Os requisitos de segurança devem ser identificados através de uma avaliação sistemática dos riscos de segurança. As técnicas de avaliação de risco poderão ser aplicadas em todas as Unidades de Negócio da Ativos ou apenas em parte delas.

Na avaliação de determinado risco, deverão ser considerados:

a) O impacto nos negócios como resultado de uma falha de segurança, levando-se em conta os potenciais consequências da perda de confidencialidade, integridade ou disponibilidade da informação ou de outros ativos da Ativos;
b) A probabilidade de tal falha realmente ocorrer à luz das ameaças e vulnerabilidades mais frequentes e nos controles atualmente implementados.

Serão feitas análises críticas e periódicas dos riscos de segurança e dos controles implementados na intenção de considerar as mudanças nos requisitos de negócio e suas prioridades, considerar novas ameaças e vulnerabilidades e confirmar que os controles internos permanecem eficientes e adequados.

Uma vez tendo sido identificados os requisitos de segurança, deverão ser selecionados e aplicados controles para assegurar que os riscos sejam reduzidos a um nível aceitável pela Ativos.

O processo de análise de riscos deverá ser periodicamente revisto, para prevenção de ameaças, inclusive àquelas advindas de novas tecnologias, visando à elaboração de planos de ação apropriados para proteção dos componentes.

8.4 Propriedade e custódia

É de propriedade da Ativos todo o seu ambiente informatizado e as informações neles contidas, que compreende todo o perímetro onde se encontram os ativos tecnológicos de processamento, armazenamento, recepção e transmissão de informações, operacionalizados em equipamentos de sua propriedade ou a sua disposição. A responsabilidade da gestão destes recursos é da Tecnologia da Informação, tendo como cogestora a unidade de negócios onde se encontram estes ativos.

Pertence ainda à Ativos toda informação armazenada, transmitida e/ ou recebidas por qualquer dispositivo e equipamentos pertencentes à empresa, ainda que não tenha sido criada em suas dependências, mas que por qualquer motivo esteja em seu poder em virtude de utilização por usuário habilitado.

A gestão da informação, que compreende sua classificação, determinação dos direitos de acesso e critérios de backup e retenção é responsabilidade do Diretor da Unidade de Negócio/Corporativo e Diretor CSC; estes poderão designar ou delegar aos subordinados a gestão e competência da Informação, mas não a responsabilidade sobre esse ativo.

A Ativos e suas Unidades de Negócios são corresponsáveis pela custódia das informações processadas em seus equipamentos e/ou armazenadas em meios eletrônicos ou não eletrônicos, localizados em suas dependências, ou em provedores contratados para a guarda.

Todos os contratos firmados que impliquem no manuseio de informações da Ativos devem conter cláusulas que garantam o cumprimento desta Política de Segurança da Informação.

8.5 Controle de acesso à Informação

O conhecimento da informação deve ser utilizado exclusivamente no desempenho das atividades profissionais ou na defesa dos interesses da Ativos.

Cada colaborador acessará apenas as informações necessárias à realização de suas funções e a ele disponibilizadas e autorizadas pelo gestor da informação, sendo responsável por cumprir os controles de segurança dela, observando todas as diretrizes da organização. Todos os acessos aos sistemas e informações da Ativos devem ser restritos apenas aos usuários autorizados, sendo:

- Restritos de acordo com os papéis exercidos pelo individuo;
- Autorizado pelo gestor responsável ou dono das aplicações;
- Revogados prontamente quando um usuário individual não necessita mais dele;
- Forçado pelos mecanismos de controle de acesso automatizado (este quando existir) para assegurar a responsabilidade individual;
- Todo acesso que não está autorizado, não está permitido.

Sempre que aplicável devem ser implementados controles de acesso físico e lógico aos ativos de informação.

Para as informações armazenadas em dispositivos eletrônicos, o acesso se dará apenas através de uma identificação pessoal e senha, sendo esta sigilosa e intransferível e cuja autorização de uso deve ser formalizada, vide Política de Gestão de Acesso a Redes e Sistemas, disponível no Portal Integra.

8.6 Segurança de Equipamentos de TI

Os objetivos da organização serão possivelmente alcançados se os equipamentos de TI forem projetados adequadamente. Essa área cobrirá o desenho dos equipamentos de TI (bem como seus ambientes), a configuração de servidores e estações de trabalho, a resiliência da instalação e sua proteção contra perdas ou danos físicos.

Os equipamentos de TI (estações de trabalho, servidores, dispositivos de rede etc.) devem estar configurados para funcionar como esperado, para prevenir atualizações incorretas ou não autorizadas, e garantir que não comprometam a segurança.

A área de Tecnologia da Informação tem autonomia para aplicar as melhores práticas de configuração de segurança nos equipamentos de TI. Para complementar uma boa configuração dos equipamentos de TI, o setor de Segurança da Informação envia periodicamente o relatório de scan de vulnerabilidades técnicas realizada nos servidores. Por sua vez, os setores responsáveis devem aplicar as configurações nos equipamentos de TI, e quando não for possível, comunicar o setor de Segurança da Informação.

Um processo deve ser estabelecido para a distribuição de atualizações (patches) de sistemas e softwares para corrigir vulnerabilidades técnicas de forma rápida e eficiente, a fim de reduzir a probabilidade de impacto nos negócios que possa acontecer.

Correções emergenciais operacionais e de segurança nos equipamentos de TI, softwares e aplicações de negócios devem ser testados, revisadas, e aplicadas de forma rápida e eficiente, de acordo com os padrões e procedimentos documentados, para responder às emergências de maneira rápida e segura, ao mesmo tempo que se reduzem os riscos à organização.

Todos os tipos de sistemas operacionais (servidores, estações de trabalho etc.) suscetíveis a códigos maliciosos, devem possuir software de proteção contra malware instalado, configurado e atualizado. Esta tecnologia visa proteger a integridade de sistemas, informações e ambientes computacionais contra códigos maliciosos que possam causar danos aos serviços.

Um processo de resposta à incidentes contra malwares para estações de trabalho e servidores na Ativos deve ser instituído. Eventos importantes relacionados à segurança da informação devem ser registrados em logs, armazenados centralizados, protegidos contra alterações não autorizadas e analisados regularmente para identificar ameaças que possam levar a um incidente de segurança, para assegurar a integridade das informações protegidas.

O gestor da área de negócio ou administradores da aplicação têm autonomia e são encorajados a solicitar que a área de segurança da informação monitore e correlacione quaisquer eventos críticos de segurança.

O registro de eventos de segurança deve ser feito em sistemas que (1) sejam críticos à organização (Ex.: dados financeiros, equipamentos críticos de rede), (2) que tenham passado por algum incidente de segurança considerável, e (3) que estejam sujeitos a legislação local e normas regulatórias.

O tempo de retenção dos logs das aplicações se dá pelo comum acordo com a área que as origina, ou detém responsabilidade pela aplicação.

Hardwares e Softwares devem ser registrados em sistemas de cadastro de ativos ou equivalentes. Licenças de software de sistemas devem ser adquiridas de forma legal por meio dos respectivos fabricantes. Seu uso deve ser planejado e uma evidência de propriedade da licença deve ser mantida.

Todos os lugares que tenham equipamentos críticos de TI, materiais críticos e outros ativos importantes devem ser fisicamente protegidos contra acidentes ou ataques.

Ambientes de produção devem estar segregados dos ambientes de desenvolvimento e de homologação.

Para uma correta cor relacionamento de eventos, todos os equipamentos de TI devem estar com seus relógios sincronizados a partir dos servidores de NTP autorizados pela Ativos. Para isso, deve haver na Ativos ao menos dois servidores internos de horário.

Este servidor deve:

- Utilizar uma versão estável e conhecida de NTP ou tecnologia semelhante;
- Buscar o horário externamente nos servidores do Observatório Nacional (ntp.br);
- Assegurar que nenhum outro equipamento além dos servidores de horário busque atualizações externas.

O scan de vulnerabilidade será realizado mensalmente pela área Segurança da Informação da Ativos, ou quando houver demanda da área responsável pelos sistemas alvo.

Mensalmente, os resultados do sana devem ser reportados às áreas responsáveis para a análise e correção das vulnerabilidades encontradas.

O scan de vulnerabilidade da Ativos tem como objetivo a análise de três camadas:

I. VM (Vulnerability Management) – gerenciamento de vulnerabilidades na camada da rede;
II. WAS (Web Application Scanning) – gerenciamento de vulnerabilidades na camada de aplicativos;
III. PC (Policy Compliance) – Gerenciamento de conformidade de configurações de padrões de segurança – Hardening.

A Ativos conta com uma solução de gestão de dispositivos móveis (smartphone, tablet etc.) para a força de vendas, cuja instalação é mandatória em todos estes dispositivos, e tem como objetivo prover:

- Gerenciamento centralizado;
- Inventário de hardware e software;
- Distribuição de aplicativos em massa;
- Rastreamento do dispositivo por geolocalização em caso de perda ou furto;
- Criptografia do dispositivo (se aplicável);
- Controle de uso de aplicativos homologados.

8.7 Segurança de Redes

Redes de computadores trafegam informações e provém um canal de acesso aos sistemas de informação. Por natureza, elas são altamente vulneráveis a interrupção dos serviços e acessos não autorizados. Manter a comunicação das áreas de negócio funcionando, exige um planejamento robusto de redes, com regras e serviços bem definidos. Esses fatores se aplicam tanto a redes locais, quanto às redes remotas (Ex.: link de unidade de negócio – VPN MPLS7 etc.), bem como comunicações de voz e dados.

A rede deve operar em equipamentos e softwares robustos e confiáveis, que sejam suportados por ambientes de contingência, para garantir que a rede esteja disponível quando necessário.

O tráfego de rede deve ser roteado através de firewall e/ou roteador, antes que qualquer acesso de entrada e saída à rede (ou sub-rede) seja concedido, prevenindo assim qualquer tráfego não autorizado.

Os acessos às centrais de administração de telefonia IP devem ser restritos, com o uso de senhas (ou equivalente), que sejam mudadas durante a instalação, para garantir que senhas padrões atribuídas pelo fornecedor não possam ser exploradas por pessoas não autorizadas e utilizadas para acessar portas que estão disponíveis para diagnósticos remotos. As orientações de segurança acima se aplicam às telefonias IP tradicionais, bem como às redes sobre voz IP (VoIP).

As estações de trabalho e servidores que podem se conectar à internet devem ser protegidas (1) usando navegadores com padrões de configuração de segurança fortes, (2) prevenindo que os usuários desativem as opções de segurança do navegador, e (3) aplicando atualizações ao navegador de maneira rápida e eficiente. Os navegadores homologados para utilização no ambiente da Ativos são: Mozilla Firefox, Google Chrome, Microsoft Edge e Internet Explorer.

Serviços de e-mail devem ser protegidos por uma combinação de políticas, procedimentos e controles técnicos de segurança para assegurar que estejam disponíveis quando necessário, a confidencialidade e integridade das mensagens estejam protegidas durante a comunicação, e os riscos em função do uso incorreto da ferramenta sejam mitigados.

O serviço de e-mail corporativo deve ser utilizado de maneira profissional, pois o uso impróprio pode comprometer a imagem da organização.

Em dispositivos móveis pessoais ou corporativos (smartphone, tablet etc.), o uso do e-mail da Ativos deve ser previamente autorizado e só poderá ser feito através de ferramenta que garanta a criptografia das informações e encapsulamento da aplicação de e-mail.

Consulte a Política de Uso de Correio Eletrônico na íntegra para o uso correto do serviço de e-mail no Portal Integra. Mecanismos de detecção de intrusões devem ser aplicados em sistemas críticos e redes para identificar novos tipos de ataques ou predeterminados. Os sistemas de detecção devem alertar o setor de Segurança da Informação sobre quaisquer comportamentos suspeitos.

O uso de equipamentos de terceiros (Ex.: prestadores de serviço) na rede de dados da Ativos deve ser identificado individualmente e autorizado pela gerência de T.I e/ou Segurança da Informação, mediante cumprimento dos requisitos mínimos de segurança da informação.

A manipulação de arquivos corporativos nos equipamentos particulares de colaboradores (ex.: disco rígido do notebook pessoal, pen drive etc.) é expressamente proibida.

O uso de equipamentos particulares (Ex.: notebooks, tablets, celulares etc.) de colaboradores para acesso à rede de dados nas dependências físicas e remotas da Ativos é proibido.

O acesso à rede remota (VPN) estão autorizados somente por meio de equipamentos corporativos autorizados e devem ser protegidos por controles lógicos (Ex.: antivírus atualizado, atualizações de segurança do sistema operacional etc.) para assegurar que estes dispositivos operem conforme os padrões definidos pela Ativos, e não comprometam a segurança de quaisquer redes as quais eles possam estar conectados.

O acesso à rede wireless deve ser autorizado, autenticado pelos usuários, e ter seu tráfego criptografado (Ex.: criptografia WPA2), para garantir que apenas as pessoas autorizadas recebam acesso, fazendo com que os riscos associados as transmissões wireless (Ex.: modificação, interceptação, monitoramento) sejam mitigados.

A Ativos deve ter uma Autoridade Certificadora para a criação, envio, e gestão de certificados de chaves públicas que são usadas para o domínio interno.

Todo e qualquer equipamento que possuir comunicação com a rede de dados da Ativos, incluindo, não devem ter seus cabos expostos, a fim de minimizar os riscos associados à intervenção física não autorizada.

8.8 Data Protection Impact Assessement (DPIA)

A Ativos deve desenvolver e manter um processo de avaliação de privacidade para DPIAs alinhados ao risco, aos requisitos legais, regulatórios e da lei geral de proteção de dados. Compete à Compliance definir o modelo e aplicar o RIPD (DPIA), nas hipóteses previstas na

respectiva política. SI apoiará, dentro de sua competência técnica (assuntos ligados à segurança da informação).

Completando a avaliação de privacidade, a área de segurança da informação fornecerá à empresa um relatório descrevendo suas descobertas, riscos potenciais e controles de mitigação recomendados.

Controles de mitigação podem ser definidos como opcionais ou obrigatórios dentro de um período. A Ativos garante que os controles de mitigação obrigatórios sejam implementados, antes do tratamento de dados ou dentro do prazo estabelecido.

A Ativos estabelece e mantém um processo para receber, avaliar e documentar a solicitação de exceção e a aceitação do risco de privacidade para circunstâncias nas quais os controles obrigatórios não são adotados.

8.9 Uso de Recursos Tecnológicos

A Ativos apenas utilizará equipamentos e softwares homologados e adquiridos legalmente de fornecedores habilitados.

Com o objetivo de garantir a gestão integrada dos ativos que acessam ou manipulam informações da Ativos e proteger a rede contra ameaças digitais, é vetado o uso de equipamentos tecnológicos particulares na rede da empresa, exceto se formalmente aprovado pelo Diretor da Unidade de Negócio, Superintendente de TI, Diretor do CSC e Corporativo.

O acesso de colaboradores da Ativos a redes públicas de computadores deve ser restrito aos interesses dos negócios e não admite qualquer manifestação de caráter pessoal.

Não serão permitidos acessos diretos aos recursos tecnológicos com usuários privilegiados e não nominais (administradores, roots, super-users). O acesso privilegiado deverá ser executado através da ferramenta de gestão de acessos privilegiados (Cofre de Senhas).

A interconexão das redes de computadores da Ativos a redes de outras empresas ou a redes públicas deve ser controlada e protegida contra invasões ou vazamento de informações, observando ainda medidas de sigilo e confidencialidade.

A Ativos pode, a qualquer momento, proceder auditoria dos acessos realizados pelos colaboradores a partir dos recursos de propriedade delas.

8.10 Guarda e Proteção das Informações

8.10.1Encriptação

É o processo de transformar a informação usando um algoritmo de modo a impossibilitar sua leitura a todos, exceto aqueles que possuem uma informação particular, geralmente referida como chave. O resultado deste processo é a informação encriptada

8.10.2Hashing

É o processo de se criar uma sequência de bits geradas por um algoritmo de dispersão, em geral representada por uma base hexadecimal, representando um nibble cada.

8.10.3Objetivos

- Proteger a confidencialidade de informações críticas (Ex: criptografia de diretórios de rede, discos rígidos, dispositivos móveis, transferências de arquivos, acessos remotos etc.);
- Determinar se as informações críticas foram alteradas (utilizando funções de hash);
- Prover uma autenticação forte para usuários de aplicações e sistemas (utilizando certificados digitais);
- Permitir que a identidade do autor de informações críticas seja identificada (usando assinaturas digitais para evitar o não-repúdio de responsabilidade).

A segurança da informação deve determinar em conjunto com as áreas de negócio a necessidade da aplicação de criptografia em diretórios de rede para proteger a confidencialidade de informações sensíveis.

A área de Segurança da Informação deve ser consultada para apoiar na definição dos protocolos para novas implementações.

As empresas fornecedoras de equipamentos e prestadoras de serviço de manutenção devem garantir a aplicação da criptografia quando solicitado pela área de T.I.

Informações armazenadas ou processadas por aplicações de negócio críticas devem ser identificadas de acordo com o seu grau de confidencialidade, integridade, disponibilidade e rastreabilidade.

8.11 Classificação da Informação:

a) Toda informação gerada e acessada no dia a dia pelos colaboradores ou em circulação pela Ativos é, em regra, confidencial, conforme o contrato de trabalho, e destinada exclusivamente para fins corporativos.

b) A informação deve ser classificada segundo os critérios abaixo:

I. **Nível 01 – Pública** – Informações aprovadas pela diretoria para uso público (interno e externo), por exemplo: relatórios anuais, indicações para a imprensa etc. Para esse tipo de informação, o armazenamento e o descarte não precisam ser controlados;

II. **Nível 02 - Restrita** – Informação não aprovada para circulação fora da Ativos como, por exemplo: memorandos internos, minutas ou atas de reuniões, procedimentos, rotinas operacionais, relatórios de projetos internos etc. A segurança neste nível deve ser controlada.

III. **Nível 03 - Confidencial** – Informações cuja circulação interna é controlada, por questões estratégicas e de gestão, onde a circulação externa é vedada, pois em caso de se tornarem públicas ou compartilhadas causarão impacto e prejuízos aos negócios da Ativos. São exemplos: planos de projetos, plantas e especificações que definem a forma que a organização opera, informações contábeis, planos de negócio, informações sobre clientes ou acionistas, entre outros. A segurança neste nível deve ser alta, restrita e deverá observar a manipulação e uso apenas por pessoas que, devido às suas atribuições, possam fazê-lo.

c) Consulte a Política de Uso correto da Informação, disponível no Portal Integra: Política de Uso da Informação.

8.12 Descarte de Documentos e Mídias

Define padrões requeridos a serem aplicados em relação ao descarte tanto de mídias quanto de dados físicos ou digitais, eventualmente contidos nos equipamentos de informática substituídos ou recolhidos pelas empresas responsáveis, bem como nos locais físicos de armazenamento definidos pela Ativos.

A destruição ou eliminação de informações deverá seguir procedimentos certificados pelas normas de segurança da informação de acordo com o grau de sigilo e importância que as informações exigirem. Consulte a Política de Descarte, disponível no Portal Integra.

A informação e os recursos físicos e tecnológicos que a suportam devem ser protegidos contra desastres físicos de cunho natural (fogo, água, calor) ou não.

As unidades responsáveis pela guarda e tratamento de informações fundamentais à continuidade dos negócios da Ativos, deve ser dotada de eficientes sistemas de controle e monitoramento de acesso de pessoas aos seus ambientes, sendo que o ingresso de colaboradores e terceiros a áreas restritas deverá ser autorizado formalmente pela pessoa com poderes para tanto.

A proteção da informação deve prevenir contra ameaças lógicas, como vírus, programas nocivos e acessos não autorizados, sejam as invasões de fonte externa ou interna. Essa proteção lógica deverá, entre outros aspectos:

- Controlar o acesso a sistemas e informações relacionadas à Ativos, indicando: qual a informação acessada, quem efetuou o acesso, qual a sua natureza e quando este acesso ocorreu;
- Garantir a segregação de funções de acordo com o perfil funcional de cada colaborador;
- Prover a administração de senhas de acesso.

O desenvolvimento de aplicações e sistemas deve ser realizado em ambiente exclusivo (homologação), distinto do ambiente de produção.

Não é permitido o uso de dados reais para testes de aplicações e sistemas em desenvolvimento, em nenhuma hipótese e sob qualquer pretexto, sob pena de arcar todos os prejuízos e, em caso de prestadores de serviços, o cancelamento dos contratos respectivos com a consequente rescisão motiva a as multas pertinentes.

É obrigatória a utilização de ferramentas antivírus, permanentemente atualizadas, em todos os equipamentos da Ativos, atitude que deve ser aliada da conduta correta dos colaboradores para evitar a contaminação do computador por vírus e/ou outros programas nocivos.

8.13 Monitoramento e Auditoria do Ambiente

Para garantir as regras mencionadas neste Política, a Ativos se reserva no direito de:

I. Instalar sistemas de proteção preventivos e detectivos para garantir a segurança das informações e dos perímetros de acesso às mesmas;

II. Implantar sistemas de monitoramento físicos e lógicos, sendo que a informação gerada por estes sistemas de monitoramento poderá ser usada para identificar colaboradores e respectivos acessos efetuados;

III. Fiscalizar qualquer arquivo que esteja na rede, no disco local da estação ou qualquer outro ambiente, visando assegurar o rígido cumprimento desta Política.

IV. Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria no caso de exigência judicial ou por determinação do Comitê Gestor de Segurança da Informação.

9 CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

Todos os colaboradores, prestadores de serviços, terceiros, jovens talentos, devem ser conscientizados dos princípios de segurança da informação, bem como entender suas responsabilidades pessoais, assegurar que os controles relevantes de segurança sejam corretamente aplicados e prevenir que as informações sejam comprometidas ou divulgadas para pessoas não autorizadas.

10 REGRAS GERAIS

Todos os colaboradores devem estar conscientes das seguintes regras:

I. É obrigatório que todos os colaboradores da Ativos recebam o treinamento de segurança da informação logo após a sua contratação. Este treinamento deve emitir um protocolo de recebimento que deve ser assinado pelo colaborador atestando ciência do treinamento realizado, que deverá ser arquivado em seu prontuário junto ao termo de responsabilidade e sigilo;

II. É de responsabilidade do contratante instruir os prestadores de serviço (terceiros) quanto a segurança da informação, devendo estar cientes das diretrizes e da política de segurança da informação da empresa e assinar o termo de responsabilidade e sigilo para terceiros quando houver solicitação de acesso aos sistemas de informação da Ativos;

III. É obrigatória a participação dos colaboradores nas campanhas e ações de segurança da informação;

IV. O significado de Segurança da Informação (Ex: proteção da confidencialidade, integridade e disponibilidade da informação);

V. A importância de concordar com as políticas de segurança da informação e aplicação de procedimentos e padrões associados a ela;

VI. Responsabilidade pessoal com a segurança da informação (Ex: avisar sobre atividades suspeitas que possam causar incidentes de segurança).

11 ÉTICA

Os colaboradores devem ser conscientizados de que são proibidos de:

VII. Utilizar informações ou sistemas não autorizados;

VIII. Uso de aplicações para propósitos que não são relacionados ao trabalho;

IX. Fazer declarações sexuais, racistas, ou quaisquer outras que possam ser ofensivas ou obscenas, discriminatórias, ou intimidadoras que possam ser ilegais (Ex: uso do e-mail, mensagens instantâneas, internet, telefone no trabalho etc.);

X. Fazer uso e/ou download de material ilegal (com conteúdo discriminatórios ou obscenos);

XI. Usar dispositivos externos não autorizados nos ativos da Ativos (Ex: softwares de terceiros, dispositivos USB, modens 3G etc.);

XII. Copiar informações ou softwares não autorizados;

XIII. Divulgar informações confidenciais (Ex: cadastro de clientes, design de produtos, políticas de preços etc.) para pessoas ou grupos não autorizados;

XIV. Comprometer senhas (Ex: Escrevendo-as em algum lugar, passando-as para outras pessoas, inclusive a área de Tecnologia da Informação);

XV. Usar informações que podem ser pessoalmente identificáveis (informações que podem ser usadas para identificar um indivíduo), a não ser que seja explicitamente autorizado;

XVI. Adulterar evidências no caso de um incidente de segurança da informação que possa requerer investigação forense.

12 PROGRAMA DE CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

Um programa regular deve ser estabelecido para promover a conscientização da segurança para todos os indivíduos que tenham acesso às informações e sistemas da Ativos, incluindo os departamentos da Matriz e unidades de negócio.
O engajamento dos líderes e gestores com o programa de segurança da informação é fundamental para promover a difusão dos conceitos de segurança da informação para os colaboradores.

13 COMPORTAMENTO PROATIVO

Comportamento pró-segurança deve ser encorajado por:

XVII. Participar obrigatoriamente dos treinamentos de conscientização de Segurança da Informação;

XVIII. Publicar os sucessos e erros de segurança dentro da organização;

XIX. Ligar a segurança aos objetivos e metas pessoais dos funcionários.

14 SEGURANÇA EM CONTRATOS DE PRESTAÇÃO DE SERVIÇOS (TERCEIROS)

XX. Todos os contratos com prestadores de serviço que envolvam o acesso, processamento e armazenamento das informações da Ativos, devem conter todas as cláusulas de segurança relevantes e obrigatoriamente o acordo de confidencialidade (NDA).

XXI. Todos os contratos de prestadores de serviço de TI (Tecnologia da Informação) devem ser analisados obrigatoriamente pelo setor de Segurança da Informação.

XXII. Para todos os outros tipos de contrato, o departamento Jurídico deve avaliar se informações críticas são transmitidas, processadas e armazenadas pelo terceiro, e, se necessário, submeter para análise e inserção de cláusulas de segurança relevantes pelo setor de Segurança da Informação.

XXIII. Os contratos de serviço que contemplem as cláusulas de segurança devem incluir no mínimo:

- Normas para assegurar a continuidade do serviço;
- Nível de serviço adequado;
- Confidencialidade da informação;
- Rastreabilidade de ponta a ponta;
- Proteção dos sistemas de informação interligados;
- E auditoria de serviços terceirizados.

Os arranjos contratuais envolvendo atividades de pagamento (TEF) entre a Ativos e os adquirentes (Bancos) devem estar atualizados e refletir as responsabilidades de cada um.

15 MESA LIMPA E TELA LIMPA

Conforme estabelecido pela Política de Uso da Informação, a política conhecida como "mesa limpa e tela limpa" são práticas recomendadas de Segurança da Informação (SI) para o ambiente de trabalho a fim de se evitar a exposição desnecessária de informações consideradas sensíveis, evitando assim o comprometimento da informação.

Visando reduzir riscos de acesso não autorizado, perdas ou danos às informações fora e durante o horário de expediente, a Ativos irão adotar a política de mesas limpas para os papéis e mídias de armazenamento removível. Outro assim, adotará uma política de telas limpas, para computadores e similares.

16 REGRAS GERAIS

Todos os colaboradores devem estar conscientes das seguintes regras:

- É obrigatório que todos os colaboradores da Ativos recebam o treinamento de segurança da informação logo após a sua contratação. Este treinamento deve emitir um protocolo de recebimento que deve ser assinado pelo colaborador atestando ciência do treinamento realizado, que deverá ser arquivado em seu prontuário junto ao termo de responsabilidade e sigilo;
- É de responsabilidade do contratante instruir os prestadores de serviço (terceiros) quanto a segurança da informação, devendo estar cientes das diretrizes e da política de segurança da informação da empresa e assinar o termo de responsabilidade e sigilo para terceiros quando houver solicitação de acesso aos sistemas de informação da Ativos;
- É obrigatória a participação dos colaboradores nas campanhas e ações de segurança da informação;
- O significado de Segurança da Informação (Ex: proteção da confidencialidade, integridade e disponibilidade da informação);
- A importância de concordar com as políticas de segurança da informação e aplicação de procedimentos e padrões associados a ela;
- Responsabilidade pessoal com a segurança da informação (Ex: avisar sobre atividades suspeitas que possam causar incidentes de segurança)

17 PROGRAMA DE CONSCIENTIZAÇÃO

Um programa regular deve ser estabelecido para promover a conscientização da segurança para todos os indivíduos que tenham acesso às informações e sistemas da Ativos, incluindo os departamentos da Matriz e unidades de negócio.

O engajamento dos líderes e gestores com o programa de segurança da informação é fundamental para promover a difusão dos conceitos de segurança da informação para os colaboradores.

A Ativos prioriza a conscientização da importância na Segurança da Informação. Assim, serão realizados periodicamente treinamentos, campanhas e outros eventos, envolvendo todos os colaboradores de todos os níveis, com o intuito de orientá-los com respeito às normas e práticas de Segurança da Informação.

18 OBRIGATORIEDADE DA POLÍTICA

O colaborador ou prestador de serviços automaticamente está atrelado a todas as regras e respectivas missivas deste instrumento e de outros que tratam de disposições corporativas, em especial as políticas, pelo que não poderá ser alegado desconhecimento frente ao amplo acesso proporcionado, seja no momento da contratação, seja pela integração respectiva ou mesmo por meio da intranet da Ativos.

O cumprimento da Política de Segurança da Informação é obrigatório a todos os colaboradores da Ativos e o seu não cumprimento representará falta disciplinar, punida de acordo com sua gravidade, nos termos da Consolidação das Leis do Trabalho, podendo acarretar, inclusive, na dispensa com justa causa do colaborador, sem prejuízo da adoção de outras medidas extrajudiciais e judiciais, cíveis e/ou criminais, necessárias para reparação do dano sofrido pela empresa e responsabilização do colaborador indisciplinado.

Todos os colaboradores têm a responsabilidade de divulgar e zelar pelo cumprimento das políticas e normas de segurança da informação, bem como, alertar os gestores de Segurança da Informação quando forem encontradas fragilidades no sistema ou nas regras estabelecidas.

Em nenhum momento será admitido a qualquer colaborador invocar o desconhecimento desta Política para justificar violações ou falta de cumprimento dela. Esta Política compromete e responsabiliza cada colaborador individualmente pelos seus atos e omissões no manuseio das informações acessadas no que tange o contrato de trabalho e afins, deixando-os ciente que os ambientes da rede da Ativos estão sujeitos a monitoramento.

Ocorrendo situações que não se enquadrem nas regras definidas nesta Política e nas respectivas normas, caberá ao Diretor da Unidade de Negócio/Corporativo e Diretor do CSC apreciar e decidir cada situação especial.

19 REVISÃO DA POLÍTICA E SEGURANÇA DA INFORMAÇÃO

Esta política, bem como todas as normas e procedimentos relacionados, deve ser revisada e reaprovada pelo Setor Segurança da Informação ao menos uma vez a cada dois anos, ou quando consideradas as seguintes circunstâncias:

- Mudanças significantes no ambiente de negócios ou estratégias corporativas (Ex.: novas prioridades de negócios etc.);
- Mudanças significantes nos riscos e no ambiente de segurança (Ex.: novas vulnerabilidades ou ameaças etc.);
- Mudanças nas obrigações legais e regulamentais, afetando o processamento de informações, governança de TI etc.;
- Incidentes significantes de segurança que impactem a Ativos.

Caso exista uma regra de segurança que caia em contradição com algum requerimento legal, a mesma deve ser revisada. Todas os documentos associados à Política de Segurança da Informação Corporativa da Ativos devem estar devidamente alinhados com ela.

A versão revisada da Política de Segurança da Informação Ativos deve ser comunicada a todos os colaboradores relevantes.

20 CONSIDERAÇÕES GERAIS

Todos os gestores são responsáveis por documento as atividades desenvolvidas em suas respectivas áreas através de Documentos Corporativos.

O colaborador é responsável e deve assegurar que o documento esteja alinhado com o Código de Ética da Ativos com os demais Documentos Corporativos existentes e com as leis e documentos vigentes. O Jurídico, Auditoria, Riscos e Compliance poderão ser consultados para auxiliarem o colaborador responsável nesta tarefa.

21 CONSIDERAÇÕES FINAIS

Esta Política é disponibilizada a todos os colaboradores da organização, através da Intranet, para conhecimento e cumprimento das diretrizes necessárias para a gestão de Compliance.

Esta Política está sujeita a revisões a cada dois anos, podendo ser revisada em periodicidade menor, caso necessário, em decorrência de alterações na regulamentação e/ou legislação aplicável ou, ainda, para refletir alterações nos procedimentos internos da Ativos.

22 PENALIDADES

O cumprimento de todas os Documentos publicados é exigido de todos os Colaboradores da Companhia constituindo-se em violação a não observância aos preceitos neles descritos, podendo acarretar a aplicação de medidas disciplinares, previstas no código de ética.

23 QUADRO DE REVISÃO

Controle de Revisões:			
Revisão	**Data**	**Área**	**Motivo da Revisão**
16	29/06/2023	Compliance	Revisão do documento

24 TERMO DE ADESÃO

ANEXO I – MODELO DE TERMO DE ADESÃO

TERMO DE ADESÃO A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA ATIVOS – ADMINISTRAÇÃO DE CARTEIRA DE VALORES MOBILIÁRIOS LTDA

Eu, [nome], [qualificação], declaro que tomei conhecimento dos termos e condições da Política de Segurança da Informação da Ativos – Administração De Carteira De Valores Mobiliários Ltda. ("Política" e "Ativos"), por meio de treinamento realizado em [•] de [•] de [•] na sede da Ativos, tendo, ao final, recebido uma cópia do Manual. Subscrevendo o presente formalizo a minha adesão ao presente Manual, comprometendo-me a cumprir com todos os seus termos e condições, adotando, nas situações de dúvida, a posição mais conservadora possível, submetendo as dúvidas a respeito do cumprimento do Manual e da legislação e regulamentação em vigor ao Diretor responsável pelo *Compliance*.

Barueri, [•] de [•] de [•].

_____
[•]

Testemunhas:

1. _____
Nome:
RG:
CPF:

2. _____
Nome:
RG:
CPF: