POLÍTICA INSTITUCIONAL & NORMAS INTERNAS

SEGURANÇA DA INFORMAÇÃO

CONGLOMERADO PRUDENCIAL:

BOLTCARD MEIOS DE PAGAMENTOS LTDA

BRASILCARD MEIOS DE PAGAMENTOS LTDA

COBUCCIO SOCIEDADE DE CRÉDITO DIRETO S.A.

COBUCCIO SECURITIZADORA DE CRÉDITOS S.A

ATUALIZAÇÃO DE VERSÕES DO DOCUMENTO

Versão	Data do Evento	Histórico	Elaboração	Aprovação
V.1	16/08/2021	Emissão do Documento	**Adriano Verola**	**Adriano Cobuccio**
V.2	18/02/2022	Revisão do documento com inclusão de normas da Lei Fed. 13.709/2018 - LGPD	Régis Martins - Compliance Adriano Verola – Seg. de Informação Raphael Antônio de Morais Ruela - Encarregado de proteção de dados	**Adriano Cobuccio**
V.3	31/05/2024	Revisão do documento	João Paulo Machado – Seg. da Informação	ADRIANO COBUCCIO:96129050615 Assinado de forma digital por ADRIANO COBUCCIO:96129050615 Dados: 2024.06.03 16:17:57 -03'00' **Adriano Cobuccio**

Versão atualizada aprovada pela Direção e arquivada no diretório de rede corporativa.

INDICE

CAPÍTULO 1 – Política Institucional

I. Disposição

A presente Política dispõe sobre as normas e procedimentos a serem observados pelas empresas que compõem o **Conglomerado Prudencial, sendo a *BoltCard Credenciadora de Cartão de Credito Ltda.***, a ***Brasilcard Meios de Pagamentos Ltda., a Cobuccio Sociedade de Crédito Direto S.A. e a Cobuccio Securitizadora de Créditos S.A. e demais empresas do Grupo Adriano Cobuccio***, no que tange a atuação de todos os Diretores, Gestores em todos os níveis hierárquicos, Funcionários e Estagiários, que tenham vínculo empregatício ou estatutário, para o cumprimento da norma de *Segurança da Informação,* baseada nas recomendações da ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação.

II. Da Direção

Responsável por garantir a efetividade e a melhoria contínua da política, dos procedimentos e dos controles internos relacionados com a aplicação da *Política de Segurança da Informação*. Ela deve prover um ambiente permanente de controle, disseminar no âmbito organizacional as melhores práticas, relacionando sempre, o programa de controle estabelecido às comunicações internas e externas e destacá-lo em apresentações para clientes e instituições com vínculos de parcerias de negócios e prestadores de serviços.

III. Dos colaboradores

É de responsabilidade de todos, do nível estratégico ao operacional, conhecer e cumprir todas as obrigações decorrentes da presente Política, bem como observar os mais altos padrões de conduta profissional ao conduzir suas atividades. Também é dever de todos os Colaboradores, informar e reportar inconsistências em procedimentos e práticas definidas no presente documento seja para seu superior imediato e/ou ao responsável direto pelo programa de controles e Prevenção a lavagem de dinheiro e do financiamento ao terrorismo da instituição.

IV. Do Responsável pelo Programa e Recursos Humanos

Garantir a efetividade de treinamentos a todos os níveis da instituição, bem como, aplicar treinamento aos novos contratados e pessoas que participem de formas diretas ou indiretas nos negócios da instituição.

V. Do Responsável pela área de TI

Garantir a efetividade nos controles e gerenciamento dos sistemas de Segurança da Informação, incluindo a Segurança Cibernética.

CAPÍTULO 2 – Normas Internas Corporativas

I. Introdução

Este documento descreve as diretrizes de segurança interna, relacionadas à segurança da informação do Grupo Adriano Cobuccio, visando garantir as três propriedades básicas das informações pertencentes ao ambiente corporativo do Grupo, descritas abaixo:

Confidencialidade: Propriedade que estabelece que a informação deva estar acessível apenas para pessoas autorizadas;

Integridade: Propriedade que estabelece que a informação esteja correta, confiável, sem a ocorrência de mudanças não autorizadas;

Disponibilidade: Propriedade que estabelece que a informação esteja sempre acessível para uso legítimo de pessoas autorizadas.

Esta política de segurança é baseada nas recomendações da norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação.

“Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio” (ABNT NBR ISO/IEC 17799:2005).

II. Objetivo desse Manual de Normas Internas

A informação é um ativo (recurso que tenha valor para companhia) de grande importância para o Grupo Adriano Cobuccio que, através de uma Política de Segurança da Informação, visa estabelecer diretrizes e padrões de comportamento de seus Colaboradores, relacionados aos ativos de dados das empresas que integram o Grupo, definindo procedimentos a serem adotados para mitigar ameaças internas e externas, tanto no meio físico quanto no meio digital.

Esse documento tem como objetivo representar as ações das empresas que compõem o Grupo Adriano Cobuccio com relação às normas internas de Segurança da Informação e nas normas vigentes no Brasil sobre o tema.

Além disso, possibilita o gerenciamento da informação do Grupo, estabelecendo normas e procedimentos específicos para orientar as condições de uso dos recursos de tecnologia, bem como implementar outros controles e processos, adequados às necessidades do negócio, que assegurem a segurança das informações manipuladas pelos Colaboradores, fornecedores, terceiros e demais prestadores de serviços do Grupo.

III. Abrangência

É destinado às empresas que que compõem o **Conglomerado Prudencial, sendo a *BoltCard Credenciadora de Cartão de Credito Ltda.***, a ***Brasilcard Meios de Pagamentos Ltda., a Cobuccio Sociedade de Crédito Direto S.A. e a Cobuccio Securitizadora de Créditos S.A. e demais empresas do Grupo Adriano Cobuccio***, levando em consideração principalmente, seus modelos de negócio, relacionamentos com os mercados e clientes.

A presente Política deve ser divulgada e formalizada a todos os Colaboradores e Terceiros com os quais o Grupo mantenha ou venha a manter relação contratual, conforme aplicável.

A Segurança da Informação é responsabilidade de toda a organização, por isso todos os Colaboradores devem assinar, obrigatoriamente, no momento de sua contratação, um termo de compromisso com esse sigilo e com a proteção dos Dados Pessoais.

IV. Definições

a) “Controlador”: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
b) “Dado Pessoal”: informação relacionada a pessoa natural identificada ou identificável.
c) “Dado Pessoal Sensível”: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

d) “Encarregado”: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

e) “Incidente de Segurança da Informação”: qualquer violação de segurança que provoque, de modo acidental ou intencional, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado a informações corporativas e/ou dados pessoais ou não.

f) “LGPD”: Lei Geral de Proteção de Dados Pessoal (Lei 13.709/2018).

g) “Operador”: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

h) “Recursos de Tecnologia (TI)”: São ferramentas de tecnologia da informação disponibilizadas aos Colaboradores para utilização a serviço da empresa, tais como, mas não se limitando a: internet, intranet, rede corporativa com seus respectivos diretórios, correio eletrônico (e-mail), Dispositivos Móveis, computadores, pen-drives, impressoras, scanners, softwares e sistemas aplicativos.

i) “Terceiro”: todo e qualquer prestador de serviços, fornecedor, consultor, cliente, parceiro de negócio, terceiro contratado ou subcontratado, pessoa física ou jurídica, independentemente de contrato formal ou não, que utiliza o nome de uma das empresas integrantes do Grupo Adriano, para qualquer fim.

j) “Titular de Dados”: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

k) “Tratamento”: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

l) “Usuário”: É todo e qualquer Colaborador, Terceiro ou visitante que utilize os Recursos de TI disponibilizados pelo Grupo Adriano.

1. Para os fins da presente Política, Dado Pessoal e Dado Pessoal Sensível serão mencionados em conjunto como Dados Pessoais. Quando existir referência a Dados, este termo engloba informações em geral, necessárias para o desempenho das atividades do Grupo, o que pode ou não incluir Dados Pessoais.

V. Procedimentos

1. RECOMENDAÇÕES

- O uso consciente e responsável dos recursos de TI deve ser aplicado a todos os funcionários do Grupo Adriano Cobuccio, tornando-os cientes dos riscos do não cumprimento das boas práticas estabelecidas por esta documentação.
- Cada colaborador é responsável pelas informações que o mesmo manipula durante a utilização dos sistemas computacionais utilizados no ambiente de TI do grupo, sendo estas restritas somente às operações internas.
- Toda Informação, confidencial ou não, é propriedade do Grupo Adriano Cobuccio, ressalvadas aquelas informações confidenciais de propriedade de Terceiros que sejam obtidas pelo Grupo através de um acordo de confidencialidade ou documento equivalente. São ativos corporativos valiosos que devem ser gerenciados com o devido cuidado.
- Todos os Dados Pessoais devem ser protegidos contra o Tratamento não autorizado ou ilegal e de situações acidentais a fim de prevenir a ocorrência de Incidentes de Segurança.
- Os Dados Pessoais devem ser utilizados exclusivamente para as finalidades mapeadas no Registro de Tratamento de Dados (ROP).
- Não é permitida a deleção de Dados Pessoais e de Informações do Grupo sem prévia autorização expressa de seu superior hierárquico, da Área de Segurança da Informação e do Encarregado.
- Quaisquer mudanças nos processos e rotinas do Grupo devem ser realizadas em conformidade com esta Política.

1.1 Acesso a informações confidenciais

O acesso a informações confidenciais ou restritas só serão autorizados quando a informação for necessária para execução de um trabalho mediante autorização do responsável pelo setor.

1.2 Acesso a informações públicas e internas

O acesso as informações públicas e internas serão autorizadas aos funcionários do grupo, visto que essas informações são de conhecimento público e de utilização do ambiente interno do mesmo.

2. CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação das informações garante que as informações sejam tratadas de forma correta durante todo seu ciclo. Essas informações podem ser classificadas utilizando rótulos que fazem referência ao seu nível de confidencialidade.

2.1 Dados confidenciais

Informações com maior nível de restrição, como informações étnicas, religiosas, senhas, informações sobre contas bancárias, etc.

2.2 Dados Setoriais

Dados que são de conhecimento somente do setor responsável pela manipulação dos mesmos. Dados como nome, endereço, cidade, e-mail, etc.

2.3 Dados internos

Dados de conhecimento interno do Grupo Adriano Cobuccio.

2.4 Dados Públicos

Dados que podem ser divulgados internamente e externamente em relação ao ambiente do Grupo Adriano Cobuccio.

3. RESPONSABILIDADES

A violação das regras de Segurança da Informação poderá acarretar sanções administrativas ou legais cabíveis.

3.1 - Deveres de Colaboradores e Terceiros:

- Tratar as informações manipuladas em concordância com as políticas de segurança atribuídas as informações de acordo com o rótulo atribuído as mesmas.

- Consultar o Setor de TI sempre que houver dúvidas relacionas à Segurança da Informação.
- Preservar a integridade e guardar sigilo das Informações e dos Dados de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações.
- Não compartilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida autorização de acesso.

- Respeitar a proibição de não copiar, instalar, usar ou armazenar programas de computador ou qualquer outro material, em violação da legislação de propriedade intelectual pertinente, ou não homologado pela área de TI.

- Comunicar ao seu superior imediato ou aos seus contatos no Grupo Adriano Cobuccio, no caso de terceiros, o conhecimento de qualquer irregularidade ou desvio, incluindo, mas não se limitando, a qualquer descumprimento ou suspeita de violação a esta Política, repassando todas as informações conhecidas sobre o descumprimento ou suspeita de violação, ao setor de TI, através do e-mail seginf@grupoadrianocobuccio.com.br, observando as diretrizes estabelecidas na Política de Respostas a Incidentes de Privacidade e Incidentes de Segurança, disponível aos colaboradores junto ao sistema interno Portal de Acesso do Grupo, com controle de acesso e para os estabelecimentos parceiros junto a Área do Lojista.

- Aos colaboradores que possuem acesso sistêmico, não compartilhar logins ou senhas, pois são de uso pessoal e intransferível.

- Tomar os devidos cuidados com o manuseio, transmissão oral e escrita de Dados Pessoais, Dados Pessoais Sensíveis e de informações confidenciais.

- Buscar auxílio da área de TI para o correto descarte eletrônico de Dados Pessoais e/ou Dados Pessoais Sensíveis contidos nas ferramentas e demais mídias utilizadas pelo colaborador. Encaminhar ao setor de Infraestrutura e Segurança para que o descarte das mídias físicas e eletrônicas seja feito de forma adequada.

- Não deixar Dados Pessoais, Dados Pessoais Sensíveis e informações confidenciais em locais com acesso irrestrito, como o diretório público do servidor de arquivos da rede

de dados que possam ser acessados por todos, ou ainda como a recepção, copa e/ou salas de reunião do Grupo Adriano.

- Dispensar atenção no momento da impressão, envio e descarte dessas informações para que outros colaboradores ou terceiros venham a ter acesso.

- Não utilizar os dispositivos e demais ferramentas disponibilizadas pelo Grupo Adriano para acessar as seguintes categorias de sites: apostas, propaganda, adultos, com material obsceno/ofensivo, atividades criminais/ilícitas, armas, violência, expressões de ódio, encontros, jogos, bate-papo (chat), sites que façam ou permitam controle remoto de computadores, hacking, sites com transmissão de som e vídeo que não sejam para fins profissionais, e outras que vierem a ser bloqueadas.

3.2 Deveres de Colaboradores com cargo de liderança:

- Cabe aos líderes de setores, tornar os Colaboradores dos mesmos, cientes das linhas gerais das políticas de segurança do Grupo Adriano Cobuccio.
- Gerenciar o cumprimento da Política de Segurança da Informação, por parte dos colaboradores sob sua gestão, garantindo a proteção das informações do Grupo Adriano Cobuccio.
- Consultar o Setor de TI sempre que houver dúvidas relacionas à Segurança da Informação.
- Identificar os desvios praticados, incluindo, mas não se limitando, a qualquer descumprimento ou suspeita de violação desta Política, e reportar a equipe de Segurança da informação, repassando todas as informações conhecidas, ao setor de TI, sobre o descumprimento ou suspeita de violação.
- Toda e qualquer solução de Tecnologia da Informação a ser contratada, deve passar pelo crivo da área de TI, que validará os aspectos de segurança, desempenho, adequação à atual plataforma tecnológica, escalabilidade, manutenção e conectividade com outras soluções.
- Garantir a assinatura de todos os colaboradores do termo de confidencialidade no momento da sua admissão.
- Garantir a assinatura de todos os colaboradores do termo de responsabilidade no momento da entrega de algum ativo de TI.

- Orientar sobre a guarda de Informações e Dados em local restrito ou em base de dados eletrônica e, em determinados casos, seu descarte, conforme recursos disponibilizados pelo área de TI para tal.
- Solicitar formalmente a liberação, alteração, suspensão ou revogação de acesso dos colaboradores e terceiros de sua equipe a qualquer recurso de TI.
- Indicar, no ato da solicitação de acesso a terceiro o prazo limite para utilização dos recursos e a data de encerramento do contrato com o terceiro.

4. GESTÃO DE PESSOAS

Cabe ao departamento de gestão de pessoas, tornar ciente os novos colaboradores, durante o período de treinamento, das linhas gerais da Política de Segurança do Grupo Adriano Cobuccio, através da documentação resumida, destinada aos mesmos.

5. DIVULGAÇÃO DAS LINHAS GERAIS DE POLÍTICA DE SEGURANÇA AO PÚLICO

Cabe ao setor de desenvolvimento do Portal de Acesso do Grupo Adriano Cobuccio, divulgar as linhas gerais da Política de Segurança no endereço http://grupoadrianocobuccio.com.br/

6. FIREWALL DE REDE CORPORATIVA

Esta seção, descreve os tipos de equipamentos de firewall utilizados e seus serviços.

6.1 Equipamentos utilizados

Para proteção do ambiente interno do grupo, são utilizados equipamentos de firewall integrados, trabalhando em HA (alta disponibilidade) que contam com recursos de balanceamento de link

6.1.1 IDS (Intrusion Detection Service)

O IDS (Sistema de Detecção de Intrusão), é uma ferramenta responsável por analisar o tráfego de entrada de rede e gerar alertas quando detecta pacotes de dados que podem fazer parte de um ataque à rede.

6.1.2 IPS (Intrusion Prevention System)

O IPS(Sistema de Prevenção de Intrusão), trabalha em conjunto com IDS, para detectar e prevenir vulnerabilidades da rede.

O IPS detecta e toma decisões em todo o fluxo de dados que entra na rede, bloqueando pacotes maliciosos assim como o endereço de origem do pacote.

O IPS utiliza os seguintes mecanismos de prevenção de ameaças:

- Monitoramento do tráfego de rede
- Identificação de atividades maliciosas
- Bloqueio de ações suspeitas
- A análise de protocolo baseada em decodificador
- A proteção de protocolo baseada em anomalias
- A correspondência de padrões com manutenção do status
- Monitoramento passivo de DNS

6.1.3 Anti DDoS (Denial of Service)

O DoS, é um ataque onde um Hacker escraviza computadores da Internet e envia requisições aos servidores até que os mesmos não consigam mais responder as outras requisições.

O serviço AntiDDoS do grupo Adriano Cobuccio impede que o tráfego malicioso atinja seu alvo, bloqueando o atacante no firewall de borda, impedindo danos aos sistemas internos do Grupo.

6.1.4 WAF (Web Application Firewall)

O WAF (Web Application Firewall) é um recurso de firewall focado na proteção dos domínios e aplicações web do Grupo Adriano Cobuccio.

Apresenta uma proteção contra-ataques de DDoS, injeção de código, ataques de brute force, enumeração de usuários, controle de sessão, controle de acesso, criptografia,

bloqueios com base em IPs maliciosos ou comportamentos maliciosos, bloqueios com base em políticas de região, horário entre outros.

6.1.5 Criptografia dos dispositivos

Todos os dispositivos da empresa deverão estar com o bitlocker habilitado, recurso que executa a criptografia dos discos impedindo que, em caso de tentativa de leitura indevida dos discos, quaisquer informações sejam acessadas por pessoa não autorizada.

6.1.6 HA – Alta Disponibilidade

A matriz do Grupo Adriano Cobuccio possui dois equipamentos que trabalham no modo espelhado, garantindo Alta Disponibilidade.

O primeiro equipamento trabalha de modo ativo e o segundo em modo passivo. Em caso de feito ou desligamento do primeiro equipamento, o segundo assume com as mesmas configurações e de modo transparente aos usuários, sem queda de internet e sem perca de acesso aos recursos da rede interna.

7. UTILIZAÇÃO DE MÍDIAS DE ARMAZENAMENTO USB

A utilização de mídias de armazenamento USB nos ativos do Grupo é bloqueada por padrão, sendo liberada pelo setor de infraestrutura somente mediante autorização da gerência e do chefe do setor a que o colaborador pertence, tornando-os cientes dos riscos oferecidos ao ambiente interno da empresa.

Todas as mídias USB que forem permitidas devem ser de uso exclusivo interno e de propriedade do Grupo Adriano Cobuccio, controlado pelo inventário de TI. É permanentemente proibido o uso de mídias não autorizadas.

8. UTILIZAÇÃO DE PASTAS DE ARQUIVO DE REDE

As permissões de acesso as pastas nos servidores de rede que contém dados setoriais e privados para colaboradores devem ser solicitadas somente pelos chefes de setor.

As permissões de acesso devem ser fornecidas visando exclusivamente o cumprimento das atividades laborais do colaborador, visando sempre o mínimo acesso necessário.

9. UTILIZAÇÃO DE SOFTWARES DE TERCEIROS

A instalação e utilização de softwares de terceiros só será permitida mediante autorização do setor de infraestrutura do Grupo Adriano Cobuccio. A instalação de softwares é bloqueada por padrão através de políticas de segurança centralizadas em um controlador de domínio AD.

10. POLÍTICAS DE SENHA

As políticas de senha devem ser obedecidas durante a criação ou troca de senhas de acesso aos computadores do Grupo, sendo essas, de uso pessoal, intransferíveis e de responsabilidades dos colaboradores.

As senhas devem obedecer aos seguintes requisitos:

- Comprimento mínimo de 8 caracteres
- Histórico de senhas memorizadas: 5 senhas
- Senhas devem conter letras maiúsculas e minúsculas, números ao menos um caractere especial
- Tempo de vida máximo da senha: 60 dias
- Duração de bloqueio de conta: 30 minutos
- Limite de bloqueio de conta: 5 tentativas incorretas

O acesso ao usuário deve ser cancelado imediatamente em caso do desligamento do mesmo do Grupo.

11. POLÍTICA DE DESLIGAMENTO DE COLABORADORES

Todo desligamento de colaboradores ou terceiros deverá ser comunicado com antecedência mínima de 24 horas ao setor de TI e Infraestrutura e de Segurança da Informação pelo Recursos Humanos ou setor responsável pela coordenação dos terceiros.

Todos os acessos deverão ser imediatamente revogados e cancelados, seja VPN, e-mail, usuário em sistemas ou quaisquer outros recursos, assim como bloqueio dos dispositivos ou equipamentos em poder do colaborador ou terceiro.

Caso haja equipamentos ou dispositivos do Grupo Adriano Cobuccio com colaboradores ou terceiros, os mesmos deverão ser evolvidos. No ato da devolução, os equipamentos ou dispositivos deverão ser avaliados e ligados apenas fora da rede ou em sandbox.

12. UTILIZAÇÃO DE E-MAIL CORPORATIVO

- O e-mail corporativo é destinado a fins profissionais, relacionados às atividades dos colaboradores;

- Os e-mails enviados ou recebidos de endereços externos poderão ser monitorados com o intuito de bloquear spams, malwares ou outros conteúdos maliciosos que violem a Política de Segurança da Informação;

- O uso de e-mails pessoais é aceitável, se usado com moderação, em caso de necessidade e quando comunicado com antecedência ao setor de infraestrutura de TI.

13. UTILIZAÇÃO DE COMPUTADORES E EQUIPAMENTOS PARTICULARES

A utilização de computadores e dispositivos pessoais só será autorizada mediante autorização da Gerência e Presidência do Grupo.

14. UTILIZAÇÃO DE PONTOS DE REDE DA EMPRESA

A utilização dos pontos de rede, onde ficam os cabos para conexão de ativos de rede, é de uso restrito aos ativos pertencentes ao GRUPO ADRIANO COBUCCIO. A utilização dos pontos de rede para conexão de ativos particulares é proibida.

15. UTILIZAÇÃO A REDE WI-FI

A criação de usuários para acesso a rede WI-FI e liberação de ativos, deve ser autorizada previamente por formulário assinado pela gerência e a presidência, tornando-a ciente dos riscos ao ambiente corporativo do Grupo.

16. CRIAÇÃO E UTILIZAÇÃO DE ACESSO EXTERNO VIA VPN

A criação de usuários para acesso externo, utilizando a VPN SSL, só será realizada com autorização prévia da presidência do Grupo. Os usuários de VPN terão seus acessos restritos somente aos recursos necessários, definidos previamente pelo setor de redes.

17. REQUISIÇÃO PARA LIBERAÇÃO DE RECURSOS DE SAÍDA DE FIREWALL

A liberação de portas de saída LAN to WAN (Saída), deve ser solicitada com pelo menos dois dias de antecedência, para que possam ser analisados os riscos provenientes da liberação solicitada, antes de ser realizada. OBS: as liberações de portas somente serão realizadas se não forem consideradas um risco ao ambiente corporativo do Grupo.

18. REQUISIÇÃO PARA LIBERAÇÃO DE RECURSOS DE ENTRADA DE FIREWALL

As liberações de portas de entrada, assim como seus redirecionamentos, devem ser solicitadas com dois dias de antecedência e devem ser de utilização restrita a sistemas de propriedade ou utilização do Grupo, assim como somente a servidores de propriedade do Grupo. OBS: as liberações de portas somente serão realizadas se não forem consideradas um risco ao ambiente corporativo do Grupo.

19. REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO

- Recursos e instalações críticas ou sensíveis devem ser mantidos em áreas seguras e com acesso restrito; além de ser fisicamente protegidos de acesso não autorizado, dano ou interferência. A proteção fornecida deve ser proporcional aos riscos identificados.
- Quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só devem ser utilizados a partir de autorização formal e mediante supervisão do superior hierárquico ou do cliente, no caso de operações instaladas no espaço físico do cliente.
- Todas as pessoas que transitarem em nossas instalações, deverão estar utilizando seu crachá de identificação.
- Em prédios corporativos, o visitante deverá estar acompanhado de um funcionário responsável.
- Documentos confidenciais deverão ser guardados em ambientes seguros e caso venham a não ter mais utilidade para a corporação, deverão ser descartados de forma correta, conforme descrito nesta Política.
- Os colaboradores que possuírem desktop ou notebook do Grupo Adriano Cobuccio, deverão ler e assinar o termo de responsabilidade.

- Componentes críticos da rede local devem ser mantidos em salas protegidas e com acesso físico e lógico controlado, devendo ser protegidos contra danos, furtos, roubos e intempéries.

20. REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO

- Os dados e os sistemas de informação são protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses dados.
- Devem ser observadas todas as diretrizes estabelecidas nesta Política, especialmente, mas não se limitando, aos seguintes aspectos: criação de usuários; senhas individualizadas; uso de equipamentos com antivírus homologado pela equipe de TI; uso de softwares homologados pela equipe de TI.
- Diariamente é feito backup dos dados.
- Caso haja algum desastre, os dados mais críticos são protegidos e replicados para garantir a continuidade dos negócios, conforme descrito no Plano de Continuidade de Negócios para Processamento e Dados em Nuvem disponível junto ao Departamento de Infraestrutura, mediante solicitação.

21. PROCEDIMENTOS DE RESPOTAS A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Em caso de incidente ou suspeita de Incidente que afete a segurança dos dados e/ou dispositivos do Grupo Adriano, o Colaborador que tiver ciência ou suspeita deve, imediatamente, seguir as determinações da Política de Respostas a Incidentes de Privacidade e Incidentes de Segurança, disponível junto ao Portal de Acesso do Grupo, e comunicar aos responsáveis para avaliação e contenção de danos. O Colaborador que não o fizer estará sujeito a sanções, incluindo medidas disciplinares e/ou judiciais, a depender da extensão e tipo de dano causado.

22. COMPARTILHAMENTO DE INFORMAÇÕES SOBRE INCIDENTES RELEVANTES

Na eventualidade de um Incidente de Segurança da Informação ou Incidente de Privacidade, deve ser observada o Procedimento Interno “Compartilhamento Sobre Incidentes Relevantes” disponível junto ao Departamento de Infraestrutura.

23. PROCEDIMENTOS DE DESCARTE/DOAÇÃO DE ATIVOS

O tratamento de ativos para o descarte será realizado por funcionários treinados do Departamento de infraestrutura do Grupo Adriano Cobuccio.

O descarte de documentos físicos deverá ocorrer de forma a garantir que as informações estejam ininteligíveis a terceiros através da destruição de documentos, a exemplo da utilização de fragmentadoras de papéis e/ou carimbos que criptografam texto escrito. É expressamente proibido o descarte de documentos que contenham dados pessoais sem que haja a destruição parcial ou total do mesmo.

Para documentos digitais, o descarte de documentos, dados e informações deverá ser feito de forma a impossibilitar a recuperação ou restauração dos arquivos, mantendo-se registros de sua exclusão

23.1 - Descarte de ativos

Processos que serão utilizados para descartar os diferentes tipos de mídia:

- Discos rígidos: abertura dos discos e destruição dos discos internos.
- Disquetes: incineração.
- Fita magnética: incineração.
- Dispositivos USB/Pen Drives: incineração.
- Cartões de memória: incineração
- CDs e DVDs: destruição da superfície da mídia e incineração.
- Documentos impressos: incineração.

23.2 - Doação de ativos

- Processos que serão utilizados para descartar os diferentes tipos de mídia:
- Limpeza completa dos documentos presentes no disco rígido do equipamento.
- Retirada de qualquer etiqueta ou outra forma de identificação do ativo na rede interna da empresa.
- Reinstalação do sistema operacional, garantindo a limpeza total dos documentos da empresa para a entrega do ativo.

24. DISPOSIÇÕES FINAIS

O conhecimento e a aprovação das regras descritas nesta Política de Segurança da Informação (PSI) possibilitarão:

- A inexistência de exceções à regra;
- Que a PSI seja um ativo estratégico;
- Que a PSI componha a política interna do GRUPO ADRIANO COBUCCIO;
- Que a PSI tenha ampla divulgação;
- Que a PSI seja incluída no processo de contratação de novos funcionários

O cumprimento das diretrizes previstas nesta Política será monitorado e fiscalizado periodicamente e em casos de descumprimento, tal fato será encaminhado para deliberação do Conselho de Administração e/ou Diretoria Executiva, bem como será contemplado no Relatório de Conformidade do Grupo Adriano Cobuccio.

As estruturas responsáveis pelas atividades relacionadas à função de conformidade possuem livre acesso às informações necessárias para o adequado exercício das suas atividades e cumprimento de seu plano de trabalho.

Esta Política entrará em vigor na data de sua divulgação, revogando e substituindo qualquer comunicação anterior sobre o assunto.

Esta Política poderá ser atualizada de tempos em tempos, de forma a estar em conformidade com as mudanças no cenário regulatório de proteção de dados e garantir a efetividade do Programa de Governança de Privacidade e Proteção de Dados do Grupo Adriano Cobuccio.