POLÍTICA INSTITUCIONAL & NORMAS INTERNAS

SEGURANÇA DA INFORMAÇÃO

CONGLOMERADO PRUDENCIAL:

BOLTCARD CREDENCIADORA DE CARTÃO DE CRÉDITO 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:96129050615 Assinado de forma digital por ADRIANO COBUCCIO:96129050615 Dados: 2021.08.09 16:44:00 -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.

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

Esse documento tem como objetivo representar as ações das empresas que compõem o **Conglomerado Prudencial e demais empresas do Grupo Adriano Cobuccio** com relação às normas internas de *Segurança da Informação*, previsto em normas vigentes no Brasil.

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.

IV. Objetivo

Possibilitar e melhorar o gerenciamento da informação do Grupo Adriano Cobuccio, estabelecendo normas, regras e padrões que assegurem a segurança das informações manipuladas pelos colaboradores e parceiros do Grupo, não dificultando o processo de negócio.

A política de segurança de informação possibilita:

- Manter a confidencialidade da informação;
- Garantir que a informação não seja alterada ou perdida;
- Permitir que a informação esteja disponível quando necessária.

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.

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

Cabe aos colaboradores encaminhar ao setor de Infraestrutura e Segurança para que o descarte das mesmas seja feito de forma adequada.

Cabe ao colaborador tratar as informações manipuladas em concordância com as políticas de segurança atribuídas as informações de acordo com o rótulo atribuído as mesmas.

Cabe aos chefes de setores, tornar os colaboradores dos mesmos, cientes das linhas gerais das políticas de segurança do Grupo Adriano Cobuccio.

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 links e recursos de segurança como IDS, IPS, Anti DDoS.

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.

6.4 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.

8. Utilização de pastas de arquivos em 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.

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, 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. 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.

12. UTILIZAÇÃO DE COMPUTADORES E EQUIPAMENTOS PARTICULARES

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

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. Procedimentos de resposta a incidentes

O Plano de Ação e de Resposta a incidentes do Grupo segue o seguinte escopo:

- Detecção: qualquer possível incidente de segurança deve ser comunicado ao departamento de Infraestrutura de TI, pelo chefe responsável pelo setor interno do Grupo, onde o possível incidente ocorreu, tornando-o ciente o Departamento de Infraestrutura de TI, para que a situação seja analisada e classificada. Esta comunicação deve ser realizada através do sistema interno de chamados do Grupo Adriano Cobuccio ou pelo ramal 3025, destinado a comunicação com os setores do Grupo Adriano Cobuccio;

- Triagem: o departamento de Infraestrutura de TI irá analisar a situação e definir se realmente se trata de um Incidente de Segurança e em caso positivo, tomar as medidas necessárias referentes ao mesmo;

- Não incidente: se a situação não se tratar de um incidente de segurança, o Departamento de Infraestrutura de TI tomará as devidas providências para resolver os problemas relatados;

- Incidente: se a situação se tratar de um incidente de segurança, o Departamento de Infraestrutura de TI deve comunicar ao Departamento de Segurança de TI para que o mesmo possa ser tratado. Esta comunicação deve ser realizada através do sistema interno de chamado do Grupo Adriano Cobuccio com prioridade máxima ou pelo e-mail seginf@grupoadrianocobuccio.com.br;

- Classificação: o departamento de Segurança de TI deverá classificar o incidente de acordo com o risco:

    - Graves: envolvem informações sobre dados sensíveis de clientes, tornado possível a identificação dos mesmos;

    - Moderados: Envolvem informações sobre dados sensíveis de clientes, porém não tornam possíveis a identificação do mesmo;

    - Baixos: envolvem informações públicas e não sensíveis;

- Atuação: após o recebimento do chamado, o Departamento de Segurança de TI atendê-lo imediatamente classificando e isolando o ativo da rede interna até que o problema seja resolvido;

- Comunicação: o Departamento de Segurança de TI deve também comunicar imediatamente a Gerência e Presidência do Grupo sobre o incidente através de memorandos destinados aos responsáveis para que o comunicado seja documentado.

- Documentação: após a resolução do problema, o mesmo deve ser documentado para registro do ocorrido.

19. COMPARTILHAMENTO DE INFORMAÇÕES SOBRE INCIDENTES RELEVANTES

Qualquer possível incidente de segurança, assim como análise de causas e impactos, deve ser comunicado ao Banco Central do Brasil sempre que solicitado.

20. PROCEDIMENTO DE DESCARTE/DOAÇÃO DE ATIVOS

O tratamento de ativos para o descarte será realizado por funcionários treinados do setor de infraestrutura da empresa Cobuccio Tecnologia.

20.1 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.

20.2 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.

VI. 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.

DocuSigned by:
Adriano Verola Viveiros
F8CA8F91C9F1416...

DocuSigned by:
Ricardo Pereira Bácule
EBEE0EF40C39455...

ADRIANO COBUCCIO:96129050615
Assinado de forma digital por ADRIANO COBUCCIO:96129050615
Dados: 2021.09.09 16:44:25 -03'00'