Galoppo

POLÍTICA DE SEGURANÇA CIBERNÉTICA

2 de dezembro de 2024

Válido a partir de	2 de dezembro de 2024
Área responsável	Compliance
Autor	Galoppo Gestora de Recursos
Contato	fmf@galoppo.com.br
Destinatários	Público em geral
Versão	2 de dezembro de 2024

SUMÁRIO

1. OBJETIVO

Serve o presente documento de Política de Segurança Cibernética da Galoppo para apresentar a avaliação de riscos potenciais sobre os ativos relevantes e o respectivo plano de resposta que os colaboradores da Galoppo devem tomar para saná-los ou amenizá-los.

As ações de proteção e prevenção visa mitigar os riscos identificados.

Os princípios que regem as Políticas de Segurança da Informação, Segurança Cibernética e Continuidade de negócios são: (i) Integridade, (ii) Disponibilidade e (iii) Proteção e, por isso, diversos procedimentos, sistemas e planos de ação destas 3 (três) políticas articulam-se entre si.

2. IDENTIFICAÇÃO DE RISCOS POTENCIAIS

RECURSO	INSTRUMENTO DE GESTÃO DE RISCOS
PESSOAS	Controle de Senhas
	Uso de correio eletrônico
	Acesso Físico a Informações e Documentos
EQUIPAMENTOS	Mapeamento de equipamentos
	Homologação de equipamentos
SISTEMAS	Utilização de Internet
	Sistemas de Prevenção a ataques externos
	Sistemas de Controle de acesso interno
INSTALAÇÕES	Segregação de Redes

3. PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA

Assim, em que pese a Galoppo possua lista com os nomes e telefones dos fornecedores de tecnologia da informação para solucionarem os problemas no menor tempo possível

em caso de necessidade, os seguintes cenários são passíveis de falha e ações de Contingência, sendo o *back office* da Galoppo o responsável direto pelas ações e manutenção:

3..1 Controle de Senhas

Todas as senhas são pessoais e exclusivas, sendo proibido o seu empréstimo, sob pena de o Colaborador ser advertido ou demitido por justa causa, além das punições administrativas e legais que couberem.

A senha deverá ser memorizada e nunca poderá ficar disposta em meios físicos ou na rede, sob pena de o Colaborador ser advertido ou demitido por justa causa, caso a senha chegue ao conhecimento de terceiros por negligência, culpa ou dolo do usuário.

As contas que ficarem sem uso por mais de 90 (noventa) dias serão bloqueadas.

O tempo para a troca obrigatória de senha é de 120 (cento e vinte) dias, sendo permitida sua modificação em prazos mais curtos.

Em caso de desligamento do Colaborador, seu login e senha serão bloqueados antes que este saiba do seu desligamento.

3..2 Normas para utilização de E-mail - Correio Eletrônico

- Cada usuário é responsável por sua conta de e-mail corporativa da Galoppo e deverá utilizá-la de forma responsável, ética e profissional.
- É proibida a utilização do correio eletrônico para envio de arquivos e divulgação de informações classificadas como confidenciais.
- É terminantemente vedado:
    - O envio de e-mail com conteúdo que contenham qualquer ameaça, calúnia, difamação, injúria, extorsão, pedidos ou aceite de propina ou qualquer outro delito previsto na legislação vigente.
    - A abertura de arquivos executáveis com os seguintes sufixos exemplificativos (.exe, .dat, dll, .com, .bat, .pif, etc).
    - O envio de correntes, Spam, ou demais conteúdos semelhantes.
    - O envio a terceiros, a qualquer título, da lista de endereços internos.
    - O envio de material com conteúdo anônimo.
    - O envio de códigos maliciosos de qualquer tipo, como, por exemplo, trojans, vírus, etc.

A Galoppo terá acesso ilimitado ao conteúdo de todas as mensagens e arquivos enviados e recebidos por seus Colaboradores utilizando a conta de correio eletrônico disponibilizada pela Galoppo.

3..3 Acesso Físico a Informações e Documentos

O princípio é impedir o acesso físico a informações e documentos classificados como sigilosos, confidenciais ou restritos para que não possam ser fotografados ou reproduzidos por algum meio digital por visitantes ou prestadores de serviço terceirizados.

Cada um dos Colaboradores será responsável pelos materiais transportados para serviço externo e impressão, sendo individualmente responsabilizado pelo eventual extravio, vazamento ou perda das informações classificadas como confidenciais.

Não é permitido deixar material classificado como sigiloso ou confidencial sobre as superfícies ou postos de trabalho após a jornada diária. Especial cuidado deve ser dispensado às informações registradas em quadros localizadas nas salas de reuniões.

Os arquivos de guarda de documentos físicos deverão ser mantidos fechados e as chaves sob guarda do responsável.

Todos os materiais com dados e informações classificados como sigilosos, confidenciais ou restritos devem ser destruídos, quando aplicável, após sua utilização.

Os materiais com dados e informações confidenciais deverão obedecer aos seguintes procedimentos para sua efetiva inutilização:

- Documentos escritos ou impressos – devem ser triturados por máquinas fragmentadoras de papel, ou na falta destas, rasgados até ficarem absolutamente ilegíveis e impossibilitados de serem reconstruídos;
- Mídias eletromagnéticas como Chips e CDs – devem ser destruídos fisicamente, se possível triturado ou, na impossibilidade, quebrados em mais de seis pedaços.

3..4 Mapeamento e Homologação de Equipamentos

Todos os equipamentos de informáticos em utilização na Galoppo e pelos seus Colaboradores deverão estar mapeados e identificados num inventário de ativos de informática. Nenhum equipamento ou sistema poderá ser adquirido, alugado ou utilizado sob empréstimo se não houver sido expressamente homologado pela Diretoria de Compliance da Galoppo.

3..5 Utilização da Internet

A utilização da Internet é, por sua natureza aberta e descentralizada, uma atividade de alto risco cibernético.

Desta forma cada Colaborador deve ter consciência que seu comportamento individual na Internet pode colocar em risco a Galoppo seus colaboradores e seus clientes.

- Os meios de controle de acesso (login e senha) à rede e à Internet devem ser rigorosamente respeitados pelos Colaboradores e Visitantes
- É rigorosamente proibido efetuar o upload de qualquer sistema, software ou dados sem autorização do Gestor TI e ou do Comitê.
- O download de sistemas da Internet somente poderá ser realizado com expressa autorização do Gestor TI e ou do Comitê, condicionado à existência de contrato de licença válido e vigente em território nacional.
- Não é permitida, sob hipótese alguma, a divulgação, facilitação ou compartilhamento de informações ou dados de interesse da Galoppo, sigilosos ou não, em fóruns, lista de discussão, salas de bate papo ou outro meio utilizando a Internet.
- O colaborador é responsável individualmente por todas as atividades que vier a realizar utilizando seu login e senha.
- É vedado o acesso à Internet fora do local de trabalho utilizando periféricos ou equipamentos da Galoppo, exceto se aprovado pela Diretoria.
- É proibido o uso de softwares de Sistemas *Peer to Peer* - P2P (Kazaa, Emule, Lime Wire, etc.).
- É expressamente proibido o acesso a sites e sistemas por meio de Proxy.

3.6 Sistemas de prevenção a ataques externos e sistemas de controle de uso interno

A Galoppo dispõe de infraestrutura de firewall fornecida pela Vivo, que tem regras de controle de acesso dos usuários com a rede pública, por meio do roteador instalado. Tal dispositivo bloqueia e mitiga o risco de eventuais acessos não autorizados em nossas redes e arquivos.

Além disso a Galoppo mantém instalado em todos os dispositivos, servidores, desktops e laptops versão atualizada do Kaspersky Small Office Security que permite:

- Verificação tem tempo real de ameaças de intrusão e vírus
- Atualização automática da base de vírus conhecidos

- Criptografia de dados nas comunicações
- Gerenciamento de políticas da Web incluindo: restrições de acesso, restrições a aplicativos, restrição de horários e restrições de sites, controle de conteúdo.

3.7 Segregação de Redes

A Galoppo manterá a rede corporativa utilizadas pelos Colaboradores fisicamente segregada da rede de acesso à internet destinada a visitantes, impossibilitando a comunicação entre ambas.

4. DEMAIS PROCEDIMENTOS

A coordenação indireta da equipe de *back office* (responsável direto) e das atividades relacionadas a este Plano de Segurança Cibernética será uma atribuição do Diretor de Compliance, a quem caberá realizar os treinamentos necessários, bem como os testes supramencionados.

A Galoppo opta por não manter equipe própria dedicada à segurança cibernética, contingência e outros assuntos relacionados com tecnologia da informação, inclusive para a realização de tarefas (e.g. instalações, substituições, configurações), verificações e manutenções periódicas.

Assim sendo, para implementação e monitoramento continuo da presente Política, a Galoppo conta com o suporte e assessoria de empresa terceirizada de tecnologia da informação.
Desta mesma maneira, a Galoppo não mantém grupos de trabalho ou outros fóruns para tratar de segurança cibernética, em que pese o *back office* seja devidamente treinado para lidar com as situações supramencionadas.

* * * * *