Política de Segurança da Informação MGC Holding

1. INTRODUÇÃO

1.1 Contexto

Esse documento visa apresentar as melhores práticas em relação a Segurança da Informação ("SI") trabalhadas pelo grupo MGC Holding, deixando claro e explícito nosso comprometimento com a Confidencialidade, Integridade e Disponibilidade das informações.

Adicionalmente, a presente Política de Segurança da Informação ("Política") visa regulamentar a cultura no tratamento de dados físicos e lógicos para que os riscos sejam mitigados; dispõe também que os Agentes de Tratamento ("Agentes") – Controladores e Operadores, devem utilizar as medidas técnicas e administrativas aptas a proteger os dados pessoais de eventuais violações.

1.2 Objetivos

A presente Política tem como objetivos (i) conscientizar o uso correto da informação, incluindo dados pessoais, dentro e fora da empresa, evitando vazamento de informações (Data Breach) ou acessos indevidos, e; (ii) proteger os direitos fundamentais de liberdade e de privacidade de acordo com a Lei Geral de Proteção de Dados ("LGPD").

1.3 Escopo

As regras que são descritas nesse documento se aplicam a todos os colaboradores do grupo MGC Holding, fornecedores e prestadores de serviço.

2. DEFINIÇÃO

A base da Segurança da Informação resume-se em três pilares: integridade, confidencialidade e disponibilidade. A partir da vigência da LGPD o controlador passou a ter a obrigação de proteger os dados pessoais que estão sob sua custódia e que estão dispostos em mais três pilares, quais sejam: acessos não autorizados; situações acidentais ou ilícitas de destruição, perda, alteração e comunicação, e; qualquer forma de tratamento inadequado ou ilícito.

Essas são as palavras-chave para a proteção à informação no meio tecnológico atual, cujos avanços trazem inúmeros benefícios, mas também, riscos à segurança de dados. Pensando nessas condições, o grupo MGC Holding desenvolveu sua Política de Segurança da Informação.

3. REGRAS

Todas as informações geradas ou utilizadas pelos recursos do grupo MGC Holding, como correio eletrônico, sistemas, aplicativos, entre outros, são de propriedade do grupo MGC Holding. Dessa forma, essas informações podem ser registradas e auditadas em qualquer meio e em qualquer momento pela corporação, sem aviso prévio.

É importante lembrar que, a responsabilidade de proteger e preservar a informação na empresa é de todos. Inclusive, qualquer pessoa que intervenha em uma das fases do tratamento obriga-se a garantir, mesmo após o seu término, a segurança da informação.

Os colaboradores poderão entender aqui nesse manual as condutas necessárias e como aplicá-las.

3.1 Acesso físico

Colaboradores

Para acessar o escritório os funcionários necessitam de um crachá para acessar o edifício e cadastro digital para acessar o escritório.

Este crachá é disponibilizado através do preenchimento de um formulário, assinado pelo responsável administrativo e assim encaminhado para a administração predial.

O cadastro da digital é realizado pela equipe administrativa.

Visitantes

Os visitantes devem se identificar na recepção do edifício e terão o acesso liberado mediante a autorização da recepção.

3.1.1 Monitoramento

Todo o monitoramento do escritório é realizado por câmeras de segurança, onde a área administrativa tem acesso à monitoria online.

Esta atividade é gerida de forma imparcial e transparente, e garante a confidencialidade das informações, preservando a identidade das pessoas envolvidas. Será dado um tratamento adequado às denúncias recebidas para investigação e resolução das irregularidades porventura identificadas.

3.1.2 Equipamentos

Nenhum equipamento de propriedade do grupo MGC Holding poderá ser retirado ou movimentado da empresa sem prévia autorização da equipe de IT.

Para tal providência será necessário a solicitação via e-mail helpdesk@mgccapital.com.br

Não é permitida a entrada de equipamentos de uso pessoal, bem como sua conexão na rede do escritório e VPN.

3.2 Acesso Lógico

3.2.1 Novos usuários

Colaboradores e Prestadores de Serviço

Solicitações de novos usuários deverão ser efetuadas através da área de Recursos Humanos via e-mail helpdesk@mgccapital.com.br, com a especificação de acessos ou usuário espelho.

Agências Externas / Escritórios de Cobrança

Obedecendo os princípios da necessidade e adequação da LGPD, solicitações de novos usuários para agências externas são feitas através de abertura de chamado (helpdesk@mgccapital.com.br), quando devem ser coletados apenas os dados necessários para a realização da atividade, a saber:

- Nome;
- CPF;
- Agência em que deve ser associado;
- Sistema que deverá acessar;

Não é permitido o acesso do usuário ao sistema legado de outro local a não ser das dependências da agência, a liberação é feita através dos IP´s de conexão informada na contratação das agências.

3.2.2 Senhas

A identificação do usuário nos ambientes e sistemas da empresa, denominada Login e Senha, é uma informação única e pessoal, a sua divulgação é expressamente proibida.

O grupo MGC Holding possui a seguinte política de senhas:

- No primeiro acesso a troca de senha é obrigatória;
- Troca obrigatório a cada 45 dias;
- Deve ter no mínimo 8 caracteres, contendo no mínimo:
  - 1 caractere alfanumérico
  - 1 caractere numérico
  - 1 caractere especial
- Não pode ser igual as últimas 6 senhas utilizadas;
- Não pode conter o login ou nome como parte da senha;

3.2.3 Acesso a Rede

Todo o compartilhamento disponível e feito através da autenticação do usuário, o perfil do usuário é definido na admissão e pode ser atualizado de acordo com as necessidades da empresa e a evolução hierárquica do usuário.

A alteração deve ser feita através de solicitações do superior imediato ou responsável pelo prestador de serviços via e-mail (helpdesk@mgccapital.com.br).

Em caso de solicitação de acesso a compartilhamento de outra área, é necessária a autorização do responsável da área afetada.

3.3 Gerenciamento

3.3.1 Atualizações de software

As atualizações de segurança e de correções são gerenciadas pelo Windows Update da Microsoft, sendo que quando as atualizações são críticas existe um prazo para que as instalações sejam realizadas.

3.3.2 Servidores

O acesso a servidores é exclusivo aos Administradores de Rede e aos responsáveis pelas aplicações quem eles rodam.

Nenhum usuário tem a permissão de logar nos servidores sem a prévia autorização de IT.

Todo e qualquer acesso efetuado nos servidores é registrado nos logs do event viewer (sistema de registro de logs e atividades) do Windows.

3.3.3 Processos

Todo e qualquer processo executado no banco de dados é monitorado 24 horas por dia, suas paradas e falhas são apontadas em relatório diário que é distribuído para o departamento de IT.

Tais falhas são verificadas e informadas para a gestão da área responsável.

3.3.4 Incidentes de Segurança

Qualquer anomalia identificada pelo usuário como: *Phishing, Pharming, Sniffing, Spoffing* etc. ou um acontecimento inesperado ou indesejado que seja hábil a comprometer a segurança dos dados pessoais de modo a expô-los a acessos não autorizados, assim como por conta de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito deve ser informada a área de IT através do e-mail helpdesk@mgccapital.com.br para bloqueio da origem do ataque em nossa ferramenta de *WebFiltering* ou *Firewall*.

Adicionalmente, quando a ocorrência do incidente de segurança relacionado a dados pessoais representar risco de dano relevante aos titulares de dados, a MGC Holding, controlador de dados pessoais, deve agir de acordo com o seu Procedimento de Resposta a Incidentes que dispõe, inclusive, a obrigação de comunicar à Autoridade Nacional de Proteção de Dados ("ANPD").

3.4 Política de uso

3.4.1 E-mail

O e-mail é uma comunicação eletrônica muito utilizada e eficaz no ambiente de trabalho. Por mais simples que pareça, essa ferramenta pode colocar em risco a segurança de dados da organização quando usada de forma indevida, para reduzir o risco dos e-mails contamos com uma ferramenta de AntiSpam do Microsoft 365, que faz uma análise antes dos e-mails entrarem nas caixas de entrada, bloqueando e-mails considerados com risco. Mesmo assim, é muito importante utilizar o e-mail de acordo com as regras de conduta:

- Não abra e-mails de origem desconhecida. Mensagem com conteúdo e remetente aparentemente verídicos pode significar riscos para seus arquivos e para as informações da empresa. Essas mensagens podem conter vírus ou instalar programas de captura de dados.

- Cuidado com anexos. Muitas vezes os remetentes são vítimas de ação de algum vírus. Previna-se! Se for necessário acessar o anexo, verifique-o utilizando o antivírus atualizado.

- Na dúvida apague a mensagem. Não corra risco desnecessário. Em caso de mensagem interna, avise a equipe de IT (helpdesk@mgccapital.com.br).

- Verifique cuidadosamente o campo destinatário para envio de mensagem. Erro no endereçamento ocasiona divulgação de informações para terceiros.

- Diga não ao Spam. Essas mensagens são utilizadas na propagação de vírus e é muito fácil reconhecê-las. Seu conteúdo vem com facilidades promocionais, propaganda enganosa, curiosidades, mensagens de amizade, entre outros títulos.

- Limpe sempre a lixeira. Não abra os arquivos que foram encaminhados para o lixo eletrônico.

3.4.2 Dispositivos portáteis

É de extrema importância que cada colaborador cuide de seus equipamentos portáteis e das informações neles contidas. Atualmente, essas ferramentas são alvos de furtos, o que pode expor informações confidenciais da empresa. Abaixo algumas orientações para garantir a segurança dos equipamentos:

- Informações confidenciais devem sempre ser armazenadas nas pastas da rede.

- Não será permitida utilização da rede corporativa por equipamento de terceiros, sejam fornecedores, clientes, equipamentos de uso pessoal ou de visitantes, exceto autorizações específicas.

- Somente os colaboradores elegíveis farão uso de equipamentos portáteis. Outras necessidades devem ser direcionadas ao diretor da área, que fará a devida justificativa e solicitação.

3.4.3 Equipamentos

Os usuários de equipamentos fixos precisam manter seus acessos seguros, evitando assim:

- Deixar o seu usuário e senha visíveis;
- Repassar seu usuário e senha para outras pessoas;
- Deixar de travar sua estação de trabalho assim que deixar a sua mesa;
- Alterar ou desabilitar as configurações de segurança do seu computado

3.4.4 Celular

Apenas pessoas autorizadas podem acessar os e-mails através de celular.

Ao configurar o e-mail no celular será obrigatório configurar uma senha de acesso ao celular para garantir a segurança dos dados.

Em caso de roubo, furto ou perda o departamento de IT deverá ser comunicado para zerar os dados remotamente do celular, e somente após comando o usuário deverá informar a operadora para bloqueio.

3.4.5 VPN

Embora o Acesso Remoto seja considerado um facilitador às informações da empresa, ele é uma porta aberta para acessos não autorizados.

Todos os funcionários do grupo MGC Holding têm acesso a VPN e devem ter algumas precauções:

- Os acessos remotos aos serviços devem ser feitos com responsabilidade e somente para propósitos autorizados.
- Todas as solicitações de acesso remoto devem ser justificadas e formalmente aprovadas pelo diretor da área.
- O acesso remoto deve ser feito através de procedimentos especiais como VPN (Virtual Private Network) e de acordo com as regras de autenticação segura.
- Evitar utilizar o acesso ao ambiente do grupo MGC Holding a partir de ambientes inseguros, como cybercafés, laboratórios de universidades, equipamentos de terceiros. Esses equipamentos podem estar infectados com programas maliciosos configurados para capturar suas informações, permitindo a um terceiro utilizá-las em uma tentativa de acesso não autorizado.

- Antes de receber o direito de acesso remoto, o usuário deve demonstrar ter conhecimentos das regras básicas de segurança e se comprometer com o cumprimento das regras definidas na Política de Segurança da Informação.

3.4.6 Impressora

Todas as impressões deverão ser retiradas no mesmo momento que solicitada, assim evitamos documentos confidenciais paradas na bandeja da impressora.

Caso ocorra algum problema na impressão devemos acionar a equipe de TI para a solução do problema e limpeza da fila de impressão pelo e-mail helpdesk@mgccapital.com.br

3.4.7 Mesa Limpa

Mesmo quando medidas acertadas e efetivas são implementadas, protegendo informações armazenadas nos sistemas (meio eletrônicos), grande parte dos problemas de segurança, especialmente os relacionados a confidencialidade, são provocados por listagens, CDs e outros meios de informação deixados desprotegidos sobre as mesas, mesmo nos horários normais de trabalho. Confira as diretrizes a seguir para evitar transtorno desse tipo e proteger as informações do grupo MGC Holding:

- Documentos, relatórios, listagens, CDs e quaisquer outros meios portáteis de informação serão trancadas em gavetas ou gabinetes, quando não em uso assistido e especialmente fora do horário de expediente normal.

- Informações críticas de negócio devem ser guardadas e trancadas. Preferencialmente digitalizá-las e salvá-las na rede da empresa.

- Um armário ou gaveta protegido por chave, ou sistema de picote de papel, devem estar sempre disponíveis respectivamente para a guarda e descarte de material confidencial.

- Se necessário, cuidados especiais devem ser dedicados ao local de armazenagem de correspondências, digitalizadoras e impressoras.

4. SUPORTE

Para qualquer tipo de ajuda ou informação, por gentileza enviar e-mail para helpdesk@mgccapital.com.br