POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

Estabelecer diretrizes, responsabilidades e procedimentos para proteger as informações do Grupo ISG contra ameaças internas e externas, minimizando os riscos à integridade, confidencialidade e disponibilidade das informações.

2. APLICABILIDADE

Aplica-se a todos os colaboradores, prestadores de serviço, consultores, estagiários e terceiros que tenham acesso aos ativos de informação, sistemas, redes e instalações do Grupo ISG.

3. PRINCÍPIOS

3.1 Assegurar que informações sensíveis estejam acessíveis apenas para indivíduos autorizados.

3.2 Preservar a precisão e a completude das informações e métodos de processamento.

3.3 Garantir que usuários autorizados tenham acesso oportuno e contínuo às informações e ativos.

4. CLASSIFICAÇÃO DA INFORMAÇÃO

As informações serão classificadas de acordo com sua importância e nível de confidencialidade:

4.1 Pública: Informações acessíveis e divulgáveis sem restrições, como conteúdo institucional ou dados já públicos.

4.2 Interna: Informações para uso exclusivo do Grupo ISG e seus colaboradores, como políticas internas e manuais de operação.

4.3 Confidencial: Informações que, se divulgadas, podem causar danos à empresa ou clientes, como dados de clientes e contratos comerciais.

4.4 Restrita: Informações críticas que, se expostas, podem comprometer seriamente a empresa, como dados financeiros e informações de segurança de sistemas.

5. CONTROLE DE ACESSO

5.1 Acesso será concedido apenas conforme a necessidade para a execução das tarefas.

5.2 Senhas devem ser claras e sérias (contendo letras maiúsculas, minúsculas, números e caracteres especiais) e trocadas a cada 90 dias, no máximo. É proibido o compartilhamento de senhas.

5.3 Todos os sistemas críticos e que contenham dados confidenciais devem adotar MFA como requisito de acesso.

5.4 Áreas sensíveis, como data centers e salas de servidores, devem ter controle de acesso restrito e registro de entradas e saídas.

6. SEGURANÇA FÍSICA E DO AMBIENTE

6.1 Computadores e dispositivos móveis devem ser bloqueados quando não estiverem em uso. Equipamentos não devem ser deixados em áreas públicas sem supervisão.

6.2 Instalações críticas devem estar protegidas contra acesso não autorizado e desastres naturais, incluindo segurança contra incêndios e controle de temperatura e umidade.

6.3 É proibido o uso de dispositivos de armazenamento externo (USB, discos externos) sem autorização prévia do setor de segurança.

7. PROTEÇÃO CONTRA MALWARE E AMEAÇAS DIGITAIS

7.1 Todos os dispositivos devem ter antivírus atualizado, além de ferramentas de proteção contra malware e ransomware.

7.2 Sistemas operacionais, aplicativos e dispositivos devem estar sempre atualizados com os patches de segurança mais recentes.

7.3 O acesso a sites não relacionados ao trabalho deve ser evitado, especialmente aqueles com conteúdo suspeito. E-mails suspeitos não devem ser abertos e devem ser reportados imediatamente.

8. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

8.1 O Grupo ISG deve manter um plano formal de resposta a incidentes com ações para detecção, contenção, erradicação e recuperação.

8.2 Todos os incidentes de segurança, incluindo tentativas de acesso não autorizado, devem ser reportados imediatamente ao setor de segurança da informação.

8.3 Após cada incidente, será realizada uma análise para identificar falhas e implementar ações corretivas, visando evitar recorrências.

9. POLÍTICA DE BACKUP E RECUPERAÇÃO DE DESASTRES

9.1 Backups de sistemas e dados críticos devem ser realizados regularmente, com cópias armazenadas em locais distintos do ambiente principal.

9.2 Backups devem seguir um ciclo de retenção que atenda às necessidades operacionais e regulatórias, mantendo cópias históricas conforme as exigências legais.

9.3 Backups devem ser periodicamente testados para garantir sua integridade e viabilidade de restauração.

9.4 Plano de Recuperação de Desastres (DRP): O DRP deve ser atualizado e testado anualmente, incluindo simulações de cenários de desastres que possam impactar as operações da empresa.

10. CONFORMIDADE COM NORMAS E REGULAMENTOS

10.1 O Grupo ISG compromete-se a proteger os dados pessoais em conformidade com a LGPD, adotando práticas de transparência, segurança e respeito aos direitos dos titulares.

10.2 Auditorias periódicas serão realizadas para avaliar a conformidade com esta política, bem como com normas externas relevantes, como ISO 27001.

10.3 Todos os terceiros e fornecedores que tenham acesso a dados da empresa devem assinar um termo de confidencialidade e estar em conformidade com as políticas de segurança.

11. TREINAMENTO E CONSCIENTIZAÇÃO

11.1 Todos os colaboradores devem passar por um treinamento inicial de segurança da informação ao ingressarem na empresa e por reciclagens periódicas, incluindo atualizações sobre ameaças emergentes.

11.2 O Grupo ISG deve realizar campanhas regulares sobre boas práticas de segurança, com conteúdo como e-mails, workshops e palestras.

11.3 Todos os colaboradores têm a responsabilidade de proteger as informações da empresa e de reportar comportamentos suspeitos.

12. AUDITORIA E MONITORAMENTO

12.1 Sistemas e redes devem ser monitorados continuamente para identificar atividades suspeitas ou potencialmente prejudiciais.

12.2 Auditorias regulares devem avaliar a eficácia das políticas de segurança, com relatórios apresentados à alta administração para acompanhamento.

12.3 Logs de acessos e atividades devem ser registrados e analisados periodicamente para identificar anomalias ou atividades não autorizadas.

13. POLÍTICA DE USO DE DISPOSITIVOS MÓVEIS E TRABALHOS REMOTOS

13.1 os dispositivos móveis devem ter criptografia de dados e proteção por senha. Dispositivos pessoais só poderão ser usados para acesso a informações da empresa mediante autorização.

13.2 Acesso remoto deve ser realizado exclusivamente por meio de soluções seguras e autorizadas, como VPN e MFA. Informações sensíveis não devem ser armazenadas em dispositivos pessoais.

14. PENALIDADES POR NÃO CONFORMIDADE

14.1 A não conformidade com esta política pode resultar em ações disciplinares, como advertências, suspensão, demissão ou ação legal.

14.2 Cada colaborador é responsável pelo cumprimento desta política e por garantir que suas ações estejam em conformidade com os padrões de segurança.

15. REVISÃO E ATUALIZAÇÃO DA POLÍTICA

Esta política será revisada anualmente ou conforme necessário para assegurar que continua adequada às ameaças e requisitos regulamentares.

O Gestor da área de segurança da informação é responsável por revisar atualizar esta política, reportando mudanças significativas à Diretoria de Compliance para aprovação.