IDG
ENGENHARIA E CONSULTORIA

POLÍTICA

SEGURANÇA DA INFORMAÇÃO

PL15

SUMÁRIO

Introdução 3

Propósito | Escopo 4

Glossário 5

Diretrizes 6

Direitos de uso 8

Deveres correspondentes 10

Proibições 12

1- Introdução

1. Introdução

A intenção por trás da publicação da Política de Segurança da Informação, não é impor restrições contrárias à cultura de abertura e confiança da IDG ENGENHARIA E CONSULTORIA, mas proteger a Empresa, nossos funcionários e parceiros, de ações ilegais ou danosas praticadas por qualquer indivíduo, de forma proposital ou inadvertidamente.

Sistemas relacionados à Internet/Intranet - incluídos, mas não limitados, os equipamentos de computação, software, sistemas operacionais, dispositivos de armazenamento, bem como seus dados, contas de rede que permitem acesso ao correio eletrônico, consultas WWW e FTP a partir de IP's (endereços de protocolo da internet) e o sistema de telefonia - são propriedades da IDG ENGENHARIA E CONSULTORIA., devendo ser utilizados com o exclusivo propósito de servir aos interesses da Empresa e de seus clientes, no desempenho de suas atividades empresariais.

A segurança efetiva é um trabalho de equipe envolvendo a participação e colaboração de todos os funcionários e afiliados de nossa Empresa que manipulam informações e/ou sistemas de informações.

É de responsabilidade da empresa divulgar e capacitar todos sob esta política e dever de cada usuário de meio eletrônico conhecer esta política e conduzir suas atividades de acordo com a mesma.

2- Propósito | Escopo

2. Propósito | Escopo

Esta política tem por propósito estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores da IDG ENGENHARIA E CONSULTORIA adotar padrões de comportamento seguro, adequados às metas e necessidades da organização.

Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação.

Resguardar as informações da IDG ENGENHARIA E CONSULTORIA, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade.

Prevenir possíveis causas de incidentes e responsabilidade legal da organização e seus colaboradores, clientes e parceiros.

Minimizar os riscos de perdas financeira, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio da IDG ENGENHARIA E CONSULTORIA como resultado de falhas de segurança.

Esta política se aplica a todos os usuários da informação da IDG ENGENHARIA E CONSULTORIA, incluindo qualquer individuo ou organização que possui ou possuíram vínculo com a organização, tais como funcionários, prestadores de serviços, consultores, auditores, fiscais e demais colaboradores que estejam a serviço da IDG ENGENHARIA E CONSULTORIA, incluindo toda mão-de-obra terceirizada ou disponibilizada mediante convênios, parcerias ou quaisquer outras formas de atuação conjunta com outras empresas; e abrange todos os sistemas e equipamentos de propriedade da ORGANIZAÇÃO, bem como aqueles de propriedade de terceiros que lhe sejam confiados a qualquer título, ou cedidos pela mesma a terceiros.

3- Glossário

3. Glossário

Ameaça: Causa potencial de um incidente, que pode vir a prejudicar a Organização.

Ativo: Tudo aquilo que possui valor para a Organização.

Ativo de informações: Patrimônio intangível da Organização, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas a Organização por parceiros, clientes, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenamento, trafegada ou transitando pela infraestrutura computacional da Organização ou por infraestrutura externa contratada pela organização, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.

Comitê Gestor de Segurança da Informação – CGSI: Grupo de trabalho multidisciplinar permanente pela diretoria da Organização que tem por finalidade tratar questões ligadas à Segurança da Informação.

Confidencialidade: Propriedade dos ativos da informação da Organização, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.
Controle: Medida de segurança adotada pela Organização para o tratamento de um risco específico.

Disponibilidade: Propriedade dos ativos da informação da Organização, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas.

Gestor da Informação: Usuário da informação que ocupe cargo específico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação.

Integridade: Propriedade dos ativos da informação da Organização de serem exatos e completos.

Riscos de Segurança da Informação: Efeito da incerteza sobre os objetivos de segurança da informação da organização.

Segurança da Informação: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da Organização.

Usuário da informação: Empregados com vínculo empregatício de qualquer área da Organização ou terceiros alocados na prestação de serviços à Organização, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar, manipular qualquer ativo de informação da Organização para o desempenho de suas atividades profissionais.

Vulnerabilidade: Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações da Organização.

4- Diretrizes

4. Diretrizes

O objetivo da gestão de Segurança da Informação da Organização é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte às operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos à instituição.

A Diretoria e o Comitê Gestor de Segurança da Informação estão comprometidos com uma gestão efetiva de segurança da Informação na IDG ENGENHARIA E CONSULTORIA. Desta forma, adotam todas as medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação às necessidades da Organização.

É política da IDG ENGENHARIA E CONSULTORIA:

• Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação da Organização sejam atingidos através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas;
• Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: Empregados, terceiros contratados e, onde pertinente, clientes;
• Garantir a educação e conscientização sobre as práticas adotadas pela Organização de segurança da informação para Empregados, terceiros, contratados e, onde pertinente, clientes;

• Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;
• Tratar integralmente incidentes de segurança da informação, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando as autoridades apropriadas;
• Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;
• Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

5- Direitos de uso

5. Direitos de uso

A Política de Segurança da Informação tem como principal objetivo documentar e proteger as informações consideradas importantes para a continuidade e manutenção dos objetivos de negócio de uma organização, padronizando e estabelecendo requisitos mínimos de segurança, atendendo diretrizes de coleta, armazenamento, compartilhamento e gestão de dados de acordo com a Lei Geral de Proteção de Dados (LGPD).

A IDG trabalha com controles e mecanismos que garantem a integridade e segurança de uma estrutura de rede na qual exista o tráfego de informações e dados comuns e/ou restritos, e nela incluídos os equipamentos que armazenam tais informações.

A IDG assegura a segurança das informações das partes interessadas e a sua própria atendendo as seguintes premissas:

• Confidencialidade: Assegura que os acessos a informações sejam obtidos, apenas, por pessoal com perfil autorizado. A quebra desse sigilo pode acarretar danos inestimáveis para a empresa ou até mesmo para uma pessoa física;
• Integridade: Assegura que a informação não seja adulterada, falsificada ou furtada;
• Disponibilidade: Assegura que a informação esteja disponibilizada sempre que solicitada pelos usuários autorizados mesmo com as interrupções involuntárias de sistemas, ou seja, não intencionais.

A Política de Segurança da Informação destina-se a todos os usuários da IDG e as pessoas que executam atividades autorizadas em nome da IDG ou de seus clientes.

Divulgar informações confidenciais ou estratégicas é crime previsto nas leis de propriedade intelectual, industrial (Lei nº 9279) e de direitos autorais (Lei nº 9610).

Os Colaboradores da IDG ENGENHARIA E CONSULTORIA, têm os seguintes direitos:

• Fazer uso legal dos recursos computacionais colocados à sua disposição, respeitadas as normas de utilização estabelecidas pela Organização;
• Ter conta de acesso à rede corporativa, respeitadas as normas de utilização e limites de acesso estabelecido pela Organização;
• Ter conta de correio eletrônico com a extensão do domínio da Organização;
• Acessar a Intranet e a Internet, respeitando as políticas da Organização;
• Solicitar suporte técnico sempre que verificado o mau funcionamento dos equipamentos ou do sistema de rede corporativa;
• Fazer uso do telefone da Empresa para tratar de assuntos relacionados ao trabalho.

6- Deveres correspondentes

6. Deveres correspondentes

Os Usuários da rede corporativa têm as seguintes obrigações:

• Responder pelo uso exclusivo de sua conta pessoal de acesso à rede corporativa;
• Identificar e nomear, classificar e armazenar, na rede corporativa, as informações e arquivos por si gerados, na forma estabelecida pelos procedimentos da ISO 9001, Procedimentos internos da IDG, SE-SQ-TB001 / SE-SQ-TB003 / SE-SQ-TB004 / PS09 3 GERENCIAR INFORMAÇÃO DOCUMENTADA.
• Zelar por toda e qualquer informação armazenada na rede corporativa contra alteração, destruição, divulgação, cópia e acessos não autorizados;
• Guardar sigilo sobre todas as informações, mantendo-as em caráter confidencial;
• Manter sigilo, em caráter confidencial e intransferível, a senha de acesso aos recursos computacionais e de informação da organização;
• Informar imediatamente ao Departamento de TI via e-mail (seginfo@idg-eng.com) e ao Comitê de Compliance, sobre quaisquer falhas ou desvios das regras estabelecidas neste documento, bem como sobre a ocorrência de qualquer situação relacionada ao trabalho, dentro ou fora das dependências da Organização.
• Responder cível e criminalmente pelos danos causados e prejuízos em decorrência da não observância das regras de proteção da informação e dos recursos computacionais da rede corporativa;
• Fazer uso dos recursos computacionais para trabalhos de interesse exclusivo da organização.

7- Proibições

É proibido aos usuários de rede:

• Não estão autorizados o uso dos recursos computacionais e demais ativos, para assuntos pessoais e/ou outras empresas/finalidades.
• Acessar, copiar, armazenar ou instalar programas de computador (Softwares) ou qualquer outro material (músicas, fotos e vídeos) que violem a lei de direitos autorais (copyright), bem como aqueles de conteúdo ilegal, pornográfico, discriminatório, homofóbico, racista ou que faça apologia ao crime;
• Utilizar os recursos de TI, colocados à disposição do colaborador em razão do exercício de sua função, para constranger, assediar, prejudicar ou ameaçar a mesma ou terceiros, sejam eles indivíduos ou organizações;
• Passar-se por outra pessoa ou esconder, por qualquer meio, a própria identidade quando utilizar os recursos computacionais ou quaisquer outros de propriedade da Organização, colocados à disposição do colaborador em razão do exercício de sua função;
• Fazer de qualquer tipo cópia ou exclusão de documento ou seu conteúdo, mesmo que em parte, armazenado nos computadores da empresa, mesmo que os mesmos tenham sido produzidos por si durante o exercício de seu trabalho. Os mesmos são de propriedade EXCLUSIVA da Empresa, respeitando os direitos autorais e de responsabilidade técnica;
• É taxativamente proibido divulgar quaisquer informações para concorrentes e/ou qualquer pessoa não ligada à Organização;
• Efetuar qualquer tipo de acesso ou alteração não autorizada a dados dos recursos computacionais pertencentes à Organização;
• Violar os sistemas de segurança dos recursos computacionais, no que tange à identificação de usuários, senhas de acesso, fechaduras automáticas, sistemas de alarme e demais mecanismos de segurança e restrição de acesso;
• Utilizar acesso discado através de modem, ou qualquer outra forma de conexão não autorizada, quando conectado à rede da Organização;
• Fazer uso do telefone da Organização para discussão de assuntos pessoais, tais como: Whatsapp, Fotos, Vídeos, Músicas, Aplicativos que não são utilizados e/ou homologados pela Organização, etc.
• Utilizar quaisquer recursos ou equipamentos da Organização para fins diversos daqueles necessários ao desempenho da função contratada;
• É taxativamente proibido a criação de Blogs e comunidades na Internet, ou qualquer ambiente virtual semelhante, sem autorização expressa da Organização;
• Realizar qualquer intervenção/alteração física nos equipamentos/ativos da organização, tais como notebooks, desktops, monitores, servidores, modens, roteadores, rede, telefonia fixa, celulares, impressoras e etc., sem a ciência do Departamento de TI.
• É taxativamente proibido acessar sites de relacionamento, redes sociais ou qualquer outro não relacionado às atividades de interesse da Organização.

8- Compromissos

Os usuários de rede comprometem-se:

• Respeitar áreas de acesso restrito, não executando tentativas de acesso às mesmas, ou utilizando máquinas alheias às permissões de acesso delimitadas a cada categoria de colaboradores;
• Não desenvolver, fomentar ou promover ações que incentivem o racismo ou qualquer tipo de discriminação que viole quaisquer outros direitos constitucionais do cidadão;
• Não fazer uso da rede para molestar, ameaçar ou ofender seus usuários ou terceiros, por quaisquer meios, sejam textos, imagens, vídeos ou correios eletrônicos;
• Não fazer uso da rede para circulação de propaganda política;
• Não tomar atitude ou ação que possa, direta ou indiretamente, indisponibilizar recursos da rede corporativa;
• Não executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilização de serviços;
• Fazer uso do telefone celular particular de forma parcimoniosa e condizente com o ambiente de trabalho, adotando um baixo tom de voz;
• Não executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da Organização;
• Não utilizar nenhum programa de bate-papo ou de mensagem instantânea, tais como Skype, MSN e Google Talk, entre outros;
• Não enviar informações confidenciais (autorizadas) para e-mails externos sem proteção. No mínimo, o arquivo deve contar com a proteção de uma senha robusta;
• Responsabilizar-se perante a Organização e terceiros por quaisquer prejuízos advindos da violação dos compromissos, deveres e proibições estabelecidas nesse documento;
• Utilizar-se, de forma ética e em conformidade com as normas de conduta e segurança estabelecidas pela Organização, de todos os recursos, equipamentos e informações que lhe sejam confiados em razão do desempenho de sua atividade profissional.

10. ADIÇÃO E REMOÇÃO DE RECURSOS

É vetada aos colaboradores da rede de computadores da organização a adição e remoção de quaisquer recursos, sejam eles microcomputadores, impressoras, pen-drives ou outros equipamentos e dispositivos. A adição e remoção desses deverão ser solicitadas ao departamento de TI, para aprovações, em caso positivo, tais procedimentos deverão ser realizados pelo mesmo.

11. AUDITORIA

Todos os colaboradores que utilizam a rede corporativa, serão submetidos a auditoria, realizada por um profissional da IDG ENGENHARIA E CONSULTORIA ou empresa especializada, com o objetivo de verificar o cumprimento das normas estabelecidas;
A auditoria ocorrerá aleatoriamente e, caso seja verificada alguma não-conformidade, será instaurada uma sindicância interna voltada à apuração de responsabilidades e classificação da gravidade da violação das normas de utilização dos equipamentos.
Após a classificação da gravidade (alta, média ou baixa), a não-conformidade será comunicada ao Comitê de Ética para adoção das providências cabíveis.

12. USO DE SENHA

Cada colaborador da IDG ENGENHARIA E CONSULTORIA deverá manter a mesma de forma sigilosa, lembrando que a senha é pessoal e intransferível. A responsabilidade pela manutenção do sigilo das senhas é exclusiva do colaborador, ao qual é proibido divulgar as senhas pessoais de acesso à rede corporativa a terceiros.

13. SANÇÕES E PUNIÇÕES

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa.

A aplicação de sanções e punições será realizada conforme análise do Comitê Gestor de Segurança da Informação, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o CGSI, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave. No caso de terceiros contratados ou prestadores de serviço, o CGSI deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato; Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano à IDG ENGENHARIA E CONSULTORIA, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos acima no tópico 14.

14. CASOS OMISSOS

Os casos omissos serão avaliados pelo Comitê Gestor de Segurança da Informação para posterior deliberação. As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação da IDG adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações da Organização.

15. REVISÕES

Esta política é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.