Política de Confidencialidade, Segurança da Informação e Cibersegurança

1. Objetivo:

A Política de Confidencialidade, Segurança da Informação e Cibersegurança ("Política") tem como objetivo estabelecer princípios e diretrizes de proteção das informações.

2. A quem se aplica a Política:

Esta Política é aplicável a todos os colaboradores das "empresas BW".

3. Regras da Política:

I - DEFINIÇÕES

I.1. Informações Confidenciais: são consideradas informações confidenciais aquelas, não disponíveis ao público, que:

- identifiquem dados pessoais ou patrimoniais
- sejam objeto de acordo de confidencialidade celebrado com terceiros
- identifiquem ações estratégicas cuja divulgação possa prejudicar a gestão dos negócios ou reduzir sua vantagem competitiva
- o colaborador utiliza para autenticação de sua identidade (senhas de acesso ou crachás) de uso pessoal e intransferível

Não se caracteriza descumprimento desta Política a divulgação de informações confidenciais quando em atendimento a determinações decorrentes do Poder Judiciário ou Legislativo, de órgãos fiscalizadores e reguladores. E quando a

divulgação se justificar, por força da natureza do negócio, a advogados, auditores e contrapartes.

I.2. Ataques cibernéticos / Cibersegurança: Os ataques cibernéticos mais comuns são:

- Malware – softwares desenvolvidos para corromper os computadores e redes, como: Vírus: software que causa danos à máquina, rede, softwares e Banco de Dados; Cavalo de Troia: aparece dentro de outro software criando uma porta para a invasão do computador; Spyware: software malicioso para coletar e monitorar o uso de informações; e Ransomware: software malicioso que bloqueia o acesso aos sistemas e base de dados, solicitando um resgate para que o acesso seja reestabelecido.

- Engenharia social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito, como exemplo: Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento; Phishing: links vinculados por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais; Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais; Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes, a fim de captar qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

- Ataques de DDoS (distributed denial of services) e botnets – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição.

- Invasões (advanced persistent threats) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

II - DISPOSIÇÕES GERAIS

Os seguintes princípios norteiam a segurança da informação:

- Confidencialidade: o acesso à informação deve ser obtido somente por pessoas autorizadas e quando ele for de fato necessário;
- Disponibilidade: as pessoas autorizadas devem ter acesso à informação sempre que necessário;
- Integridade: a informação deve ser mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

As seguintes diretrizes devem ser seguidas por todos os colaboradores:

- As informações confidenciais devem ser tratadas de forma ética e sigilosa e

de acordo com as leis e normas internas vigentes, evitando-se mau uso e exposição indevida.

- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.
- A concessão de acessos às informações confidenciais deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades.
- A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.
- Segregação de instalações, equipamentos e informações comuns, quando aplicável.
- A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.
- Qualquer risco ou ocorrência de falha na confidencialidade e na segurança da informação devem ser reportados ao responsável pelo Compliance.

III - PROCESSOS E CONTROLES

Controles de Segurança da Informação Confidencial

Para assegurar que as informações confidenciais sejam adequadamente protegidas, as Empresas “BW” definiram os seguintes processos / controles:

Identificação da Informação

O colaborador que recebe ou prepara uma informação deve identificar a natureza desta, conforme o item a seguir.

Classificação da Informação

As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Confidencial, Restrita e Pública.

Para a classificação devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

Controles para informações classificadas como “Confidencial”

Informações confidenciais devem ser identificadas como tal: e-mails, apresentações, documentos.

Os e-mails e arquivos com informações confidenciais devem ser protegidos.

O acesso às informações confidenciais deve ser controlado.

Qualquer documento pessoal que seja disponibilizado a terceiros deve ser enviado com a identificação do terceiro, editada em marca d'água.

Sempre que necessário, contratos de confidencialidade da informação devem ser assinados com terceiros.

Controles Gerais de Segurança da Informação e Cibersegurança

Salvaguarda da Informação

A informação deve receber proteção adequada em todo o seu ciclo de vida, que compreende: Geração, Manuseio, Armazenamento e Descarte.

O colaborador, responsável pela informação gerada, deve ter conhecimento do tempo regulatório de salvaguarda e gerenciar o seu armazenamento e descarte.

Na dúvida do tempo regulatório, questionar o Jurídico.

O descarte de informação confidencial deve ser efetuado utilizando máquina fragmentadora de papéis ou incineradora.

Mesa Limpa

Nenhuma informação confidencial deve ser deixada à vista.

Ao usar uma impressora coletiva, recolher o documento impresso imediatamente.

Gestão de Acessos

Controles de Gestão de Acessos, que devem ser garantidos por Tecnologia da Informação:

- Definição de regras para senhas de acesso aos sistemas corporativos, prevendo inclusive a troca periódica das mesmas.
- Definição de perfil de acesso aos sistemas internos e externos de colaboradores, terceirizados e prestadores de serviços, principalmente às informações confidenciais.
- Controle dos acessos de colaboradores, terceirizados e prestadores de serviços em caso de desligamento e encerramento das atividades.
- Os acessos físicos e do ambiente corporativo, inclusive por meio remoto e por meio de dispositivos pessoais como celulares, devem ser rastreáveis, a fim de garantir que todas as ações sejam passíveis de auditoria e possam identificar individualmente o Colaborador, para que o mesmo seja responsabilizado por suas ações.
- Os equipamentos, ferramentas e sistemas concedidos aos colaboradores devem ser homologados e configurados com os controles necessários para cumprir os

requerimentos de segurança aplicáveis às “Empresas BW”.

Controles de Segurança Física e controles de acesso às instalações, que devem ser garantidos pela área Administrativa:

- Controle de acesso por meio de crachás e filmagens.
- Espaço físico adequado e restrição de acesso para a guarda de equipamentos e informações confidenciais.
-

Cibersegurança

Controles de Cibersegurança, que devem ser garantidos por Tecnologia da Informação:

- Proteção dos dados armazenados, contendo ferramenta segura de backup e criptografia, conforme necessário; bancos de dados e dispositivos de rede devem ser enviados para um sistema de segurança dedicado que seja rigorosamente controlado para preservar a integridade, a confidencialidade e a disponibilidade do conteúdo;

- Uso de assinaturas digitais para alguns processos/colaboradores críticos;

- Atualização dos sistemas operacionais e softwares utilizados na instituição;

- Prevenção de ameaças com firewalls, antivírus, perfis de acesso específico para os administradores das máquinas, filtros de spam, controle para uso de periféricos (pendrives, CDs e HDs), DLP, FireEye e filtros de uso de internet;

- Inclusão das preocupações de segurança durante as fases de desenvolvimento de novos sistemas, softwares ou aplicações;

- Controles de auditoria, tais como sistemas de gerenciamento de senhas, logs e trilhas de acesso;

- Controle de acesso e CFTV no ambiente do CPD.

- Contrato de manutenção com Suporte 24x7 dos Servidores.

Gestão de Riscos

A Gestão de Riscos inicia com uma avaliação de riscos e a implementação de controles baseados nos riscos, levando em consideração o ambiente de controle da Empresa, suas atividades, processos e clientes. A avaliação de riscos deve ser atualizada de forma a identificar novos riscos, ativos e processos.

A avaliação de riscos segue a metodologia do Risco Operacional, conforme respectiva Política.

A gestão de Riscos deve contemplar monitoramento e testes com o objetivo de detectar as ameaças e reforçar os controles, bem como criação de Plano de Resposta que é o planejamento prévio para tratamento e recuperação de incidentes, incluindo um plano de comunicação.

Tratamento de Incidentes de Segurança da Informação,

Os riscos e incidentes de Segurança da Informação devem ser reportados ao Responsável pelo Compliance, que analisará caso a caso e adotará as medidas cabíveis.

Back ups, Plano de Contingência e Continuidade de negócio

Plano de contingência e de continuidade dos principais sistemas e serviços deverá ser implantado e testado no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Os mesmos controles de segurança e controle de acesso devem ser aplicáveis nas instalações do site de contingência.

Deve haver back up e que os mesmos sejam testados anualmente.

Testes de Controles

A efetividade da política de Confidencialidade e Segurança da Informação deve ser verificada por meio de testes periódicos dos controles existentes

Um plano de teste deve ser efetuado pelo responsável por Tecnologia da Informação assegurando que:

- recursos humanos e computacionais estejam adequados ao porte e as área de atuação,
- adequado nível de confidencialidade e acessos as informações confidenciais,
- segregação física e lógica,
- recursos computacionais , de controle de acesso físico e lógico, estejam protegidos,
- manutenção de registros que permita a realização de auditorias e inspeções.

Propriedade Intelectual

Tecnologias, marcas, metodologias e quaisquer informações que pertençam as Empresas “BW” não devem ser utilizadas para fins particulares, nem repassadas a

outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho.

Rastreamento

É permitido o uso pessoal dos equipamentos de informática e de comunicação utilizados pelos colaboradores para a realização das atividades profissionais. Lembrando que como tais recursos, como e-mails, sistemas, computadores, telefones e gravação de voz pertencem às Empresas "BW" , são rastreáveis e sujeitos a monitoramento, bem como podem se tornar públicos em caso de auditoria e/ou exigência judicial.

O acesso interno às informações e gravações deve ser previamente autorizado pelo "Head da área" e copiado o responsável pelo Compliance.

Termo de Conhecimento

Os Colaboradores devem aderir formalmente a um termo, comprometendo-se a agir de acordo com a política de Segurança da Informação.

Treinamento

Os colaboradores que tenham acesso a informações confidenciais ou participem de processo de decisão de investimento devem ser treinados a respeito de Segurança da Informação.

Todos os colaboradores devem ser treinados em Cibersegurança

4. Responsabilidades:

Os colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política, informando qualquer irregularidade ao responsável por Compliance, a quem caberá avaliar e submetê-las ao Conselho de Ética, que tomará as medidas cabíveis.

O canal de comunicação e denúncia para o assunto é o Compliance

A Área de Tecnologia da Informação é responsável pela implementação dos procedimentos e controles técnicos inerentes a esta Política, bem como pelos testes de controle, podendo ser realizados por terceiros, indepentes.

O Responsável pelo Compliance deve garantir o atendimento a esta Política, bem como a dfusão de uma cultura de segurança nas Empresas.

.

5. Contato:

Para maiores informações e/ou dúvidas, entrar em contato com o Responsável por Compliance.

Termo de Conhecimento da Política de CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

NOME		
ÁREA	*CARGO*	
DOC. IDENTIDADE Nº	*TIPO*	*CPF*

Declaro que tenho conhecimento da Política de CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO e que estou ciente do seu teor, o qual está diretamente ligado ao exercício de minhas funções.

De acordo com este termo, comprometo-me a:

a) Adotar e cumprir as diretrizes indicadas na política;

b) Comunicar imediatamente responsável por Compliance qualquer violação dessa política que venha a tornar-se do meu conhecimento, independente de qualquer juízo individual, materialidade ou relevância da violação.

Estou ciente de que meus acessos físicos, lógicos, de voz e de imagem podem ser objeto de monitoramento.

Desde já, aceito incondicionalmente, sempre que solicitado, atender e cumprir quaisquer novos itens e condições que possam vir a ser considerados partes integrantes desta Política, sem a necessidade de apor assinatura em novo termo, bem como em caso de negligência ou imprudência na aplicação desta Política, tenho total ciência da responsabilidade disciplinar que recairá sobre tal inobservância.

_____, _____ de _____ de 20_____

(local)

_____

Assinatura do Colaborador