CAPITÂNIA S/A

Política da Segurança da Informação

A Política de Segurança da Informação é o conjunto procedimentos que devem ser seguidos para preservar a segurança, integridade e confidencialidade da informação sob gestão da Capitânia

I- Acesso aos Recursos de Informação

1. **Senha de Login na Rede**: Pessoal e intransferível.

    a. Cada usuário é responsável por todas as atividades realizadas por intermédio de sua senha de acesso.

    b. Troca de senha requerida a cada 45 dias.

2. **Acesso às Pastas:** Todo arquivo de trabalho deve estar em uma das pastas do servidor central. Arquivos de trabalho no drive local (C:) não são permitidos, com exceção do arquivo .pst do Microsoft Outlook, por razões técnicas.

3. **Programas**: Todo programa só pode ser instalado pela área de Tecnologia.

4. **Equipamentos:** Todo equipamento (monitores, computadores, laptops notebooks, switches, roteadores, caixas de som, wifi, impressoras entre outros) só pode ser instalado pela área de Tecnologia.

5. **E-mail:** Deve ser utilizado apenas para atividades profissionais.
   Pastas de e-mail diferentes da Inbox (“pastas pessoais” no jargão Microsoft) devem ser armazenadas na rede, no diretório U: (“usuários”), sob a pasta pessoal.

6. **Acesso à Internet:** Deve ser utilizado apenas para atividades profissionais. Proibido:
    a. o acesso a conteúdo pornográfico, jogos, relacionamentos, conteúdo de hackers, proxys, conteúdo racista ou discriminatório de qualquer natureza.

    b. a utilização de softwares P2P e torrent como Emule, Kazaa, Vuze e outros.

    c. Download de filmes, músicas, seriados, jogos, softwares.

   O acesso à Internet é monitorado e sujeito a filtros de conteúdo.
   Qualquer liberação de acesso a sites deverá ser feita por escrito e estará sujeita a aprovação da área de Tecnologia e Gerente de Área.

7. **Skype:** Apenas Contas Designadas têm acesso autorizado ao Skype.
   É proibido:
   a. Postar mensagens de cunho discriminatório, difamatório, ou de qualquer maneira ilegal;
   b. Representar a Capitânia fora da função específica a que se destina.

8. **Pen Drive:** Apenas Usuários Designados têm pen-drive liberado.

9. **CD-ROM:** Apenas Usuários Designados têm dispositivo de gravação e leitura habilitado.

10. **Dispositivos de impressão:** há um dispositivo de impressão por área. Cada estação deve mapear exclusivamente o dispositivo de impressão da sua área, exceto as Usuários Designados para ter acesso à impressora de alta qualidade

11. **Impressora de Alta Qualidade**: Localizada na Administração. Apenas Usuários Designados podem mapear esta impressora. Uso da mesma requer preenchimento da pauta fazendo constar quem usou, para que área, projeto, e número de páginas.

12. **Acesso remoto à rede da Capitânia (VPN):** Apenas Usuários Designados podem ter acesso à VPN. Dada potencial vulnerabilidade da estação remota, o uso deve ser parcimonioso.

13. **Celular**: Membros da atividade de Gestão de Recursos não podem usar celular na mesa.

14. **Usuários Designados**: São aqueles listados no Anexo A.

II- Política de Backup

1. **Serviços de backup** são:

   a. backup InSite, incremental, criptografado, diário por 12 meses, com finalidade de recuperar arquivos acidentalmente perdidos.
   São utilizados backup em fita e em Disco Rigido para uma melhor tolerância a falhas.

   b. Backup para o Site de Contingência: diário, para site remoto, via VPN, com a finalidade de restaurar operação após parada do site principal.

   c. Backup OffSite: backup para disco rígido removível e fita LTO (criptografado, protegido por senha), armazenado em dois locais diferentes do site principal e do site de contingência.

d. Backup de e-mail no servidor: realizado em ambiente cloud protegido por senha e aplicação própria de comunicação entre servidor e caixa de email (comunicação em túnel). Sistema de backup de mensagens sem limite de tamanho e número de mensagens**.**

2. Os arquivos PST dos usuários são copiados semanalmente para um disco rígido externo criptografado e armazenado em local diferente do site de contingencia e do site principal.

3. Em nenhuma circunstância os equipamentos de Backup OffSite e site de Contingência poderão estar ao mesmo tempo no site principal. Para uma total reestruturação após evento catastrófico deverá ser utilizado sistema de rodizio para reestabelecer o ambiente.

III-Plano de Continuidade de Negócios

Planos de contingência:

Plano	Descrição
1. Link de Contingência	Link de internet redundante acionado automaticamente em caso de queda do link principal eainda trabalhando em paralelo para que não haja um estrangulamento de conexão.
2. Contingência de e-mail	Contas de e-mail hospedadas em ambiente Cloud com 99,995% de uptime garantido por contrato.
3. Queda de energia	No-breaks instalados em todas as maquinas e servidores e em caso de queda, um gerador assume a distribuição de energia.
4. Site de Contingência	Site independente em caso de disrupção grave do site principal. Site independente com copias de segurança dos arquivos do site principal.
5. Telefonia	Alem das linhas telefônicas contratadas (E1) existem ainda linhas externas independentes do PABX ligadas ao gerador

1. **Site de Contingência-** Está localizado distante do site principal e será composto de:
   a. Instalações físicas para 4 estações;
   b. Acesso banda larga à internet com firewall;
   c. Pelo menos 2 linhas telefônicas;
   d. Servidor sincronizado com o site principal, com defesas contra acesso não autorizado (senha de criptografia e firewall);

e. rede para pelo menos 4 estações.
f. Impressora
g. Pelo menos 1 desktop além do servidor.

2. **Serviços do Site de Contingência** contam com no mínimo:
   a. Sistema SMA
   b. Capitânia Mailer
   c. Arquivos Administrativos
   d. Arquivos que possibilitam a continuidade dos trabalhos da empresa, tais como planilhas e documentos

3. **Serviços Remotos de Contingência** acessíveis remotamente serão:
   a. E-mail (webmail e smartphone)

4. **Rotinas essenciais**: a serem executadas do site de contingência:
   a. Envio diário de cota para investidores
   b. Boletagem SMA
   c. Trabalhos referentes ao *"core business"* da empresa.

5. **Ordem de Ativação**:

   a. Com queda da energia do site principal antes que as rotinas essenciais tenham sido completadas, faz-se ativação dos no-breaks automaticamente e antes que a bateria dos mesmos seja exaurida, o gerador deverá assumir a distribuição de energia.

   b. O site de contingencia (remoto) deve ser ativado se:

      i. Houver impossibilidade física de acessar o site principal; ou

      ii. Não houver possibilidade de ligação à internet no site principal (nenhum dos links, principal ou contingência, e nenhum meio viável de acesso por modem de celular); ou

      iii. A manutenção do site principal sob queda de energia tiver atingido o limite máximo dos nobreaks e gerador; ou

      iv. Rotinas necessárias envolverem os servidores e estes não estiverem disponíveis.

6. **Procedimento de Ativação – Site Contingencia.**
   a. Mover para o site de contingência o número necessário de pessoas com laptops (menos 1 estação já provida no site)
   b. Conectar na rede (usar rede wireless se o número de conexões passar de 4) – atenção para a senha de conexão de rede wireless disponível no site.
   c. Mapear as pastas do servidor de contingência conforme necessário.

IV- Rotinas de Testes

7. Teste do site de Contingência:

    a. Aleatoriamente, com frequência esperada trimestral, as rotinas essenciais (liberação de quota, SMA) deverão ser feitas do Site de contingencia.

8. Teste de gravação de Telefonia:

    a. Diariamente, será verificada a taxa de gravação dos arquivos à procura de anomalias (arquivos crescendo rápida ou lentamente demais);

    b. Semanalmente, deve ser testada a gravação nas salas de reunião;

9. Teste de No-Break e Gerador

    a. Bimestralmente a energia do escritório deverá ser cortada para se verificar a disponibilidade e autonomia dos nobreaks e gerador

    b. Semestralmente será feita manutenção preventiva nos equipamentos de energia ou caso algum deles apresente defeito nos testes bimestrais.

    c. Semestralmente o gerador deverá ser verificado quanto ao seu reservatório de combustível

10. Teste de equipe de segurança

    a. Mensalmente e em horários aleatórios o alarme deverá ser disparado para verificar o tempo de resposta e qualidade de reposta, visto que nem sempre a contra-senha será fornecida.

    b. Trimestralmente um funcionário aleatório em um final de semana deverá acessar o prédio sem que seu nome esteja na lista de permissões.

11. Teste de Backup

    a. Mensalmente o backup deverá ser recuperado (restore) de uma pasta selecionada aleatoriamente.

    b. Semestralmente deverá ser feito uma recuperação completa dos arquivos da empresa.

12. Alteração de senhas de acesso

    a. Bimestralmente as senhas de acesso aos conjuntos deverão ser alteradas.

V- Gravação de Comunicações

1. A CAPITÂNIA monitorará o trafego de informações através de suas redes de comunicação, ou seja, telefonia, internet e correio eletrônico.

2. Os ramais de telefonia gravados são:

    a. Todos os Ramais

3. O conteúdo das gravações será transferido do servidor de gravação para:
    a. HD externo removível criptografado protegido por senha com periodicidade de 6 meses.
    b. Unidade de fita de backup para armazenamento offsite
    c. DVD-R para armazenamento offsite

4. O acesso a gravações só pode ser realizado com permissão da pessoa gravada, ou quando exigido por lei.

5. Comunicações via Skype são gravadas em pasta na rede por programa residente específico.

6. Os acessos feitos pela internet são gravados pelo servidor, com identificação do usuário que acessou e o destino acessado.

VI- Segregação de Informação

1. **Áreas de Segregação:** As seguintes são áreas estanques:
    a. Consultoria
    b. Gestão de Carteira

2. **Licenças:** A Consultoria opera sob licença de Consultor de Valores Mobiliários; Gestão de Carteira opera sob licença de Administrador de Carteiras de Valores Mobiliários; ambas emitidas pela CVM.

3. **Segregação Física**: Cada área se comunica única e exclusivamente com o Hall de saída (Recepção / Elevadores). Não existem janelas, salas de reunião ou visita ou outras áreas comuns. As salas de visita constituem bloco à parte ligado à Recepção e ao Hall de saída. Cada uma das áreas fica em um conjunto separado com porta com senha própria

4. **Segregação Lógica**: as partições do servidor de arquivo terão acesso exclusivo por área e por perfil de usuário.

5. **Mapeamentos:**

    A pasta N: (sistemas) é de uso comum e deve conter exclusivamente material comum (pesquisa, biblioteca, acesso ao Bloomberg). Quaisquer arquivos estranhos a estas denominações deverão ser movidos para suas pastas especificas sob o risco de serem deletados.
    - Pasta Geral sem informação sensível

    Os equipamentos de roteamento (*switches*, roteadores, *hubs*) que servem cada área devem ser independentes.

6. **Segregação Funcional:** associados não podem ter função em mais de uma área.

7. **Segregação de Informações**: associados de uma área não podem trocar informações confidenciais, proprietárias ou não-públicas da área com associados de outra área.

VII- Revisão da politica

1. Todas as políticas acima listadas deverão ser revistas em um prazo máximo de 12 meses após a conclusão de sua aplicação.

    a. Tal revisão deverá ser feita com o intuito de atualizar a mesma aos novos riscos apresentados durante o período por uma série de fatores, sejam eles comportamentais (novo tipo de celular, óculos inteligentes, discos externos etc..), físicos, cibernéticos (ataques a roteadores, impressoras

ou novas modalidades de ataques a servidores) ou por conta de políticas empresariais e de compliance.

VIII- Treinamento

1. **Corporativo**: É obrigatório treinamento interno em segurança da informação, negociação por detentores de informação privilegiada, e segregação de informação, pelo menos uma vez por ano. A freqüência é obrigatória. Cada participante deve assinar uma declaração de que participou do treinamento, conforme modelo no Anexo B.

2. **Corporativo de TI**: Treinamentos recorrentes das melhores práticas de segurança, novidades e mudanças na área de TI que poderá influenciar diretamente os funcionários.

3. **Equipe de TI**: Treinamento e atualização da equipe de TI em termos de melhores práticas de segurança, recursos e novidades.

ANEXO A

Usuários Designados

Nome	Pen-Drive	Gravação CD/DVD	VPN	Impressora Qualidade	Partição Administrativa		
Ricardo Quintero (quintero)	X	X			X		
César Lauro (clauro)	X	X		X	X		
Margareth Brisolla (mbrisolla)	X			X	X		
Arturo Profili (arturo)	X	X		X			
Flávia Krasupenhar (flavia)	X	X					

ANEXO B

Modelo de DECLARAÇÃO DE PARTICIPAÇÃO

DECLARAÇÃO DE PARTICIPAÇÃO NO TREINAMENTO INTERNO DE SEGURANÇA DA INFORMAÇÃO

Eu, abaixo assinado, participei do Treinamento Interno de Segurança da Informação, versando sobre segurança da informação, confidencialidade, negociação por pessoas detentoras de informações privilegiadas, e segregação de atividades, oferecido pela Capitânia em ....., e me comprometo a aderir às melhores práticas apresentadas.

São Paulo, _____ de _____ de _____

ASSINATURA:

NOME: