

GRID

INVESTIMENTOS

ASSESSOR DE INVESTIMENTO

Política de Segurança da Informação

Elaboração: GRID

Aprovação: Priscila Navarro

Versão: V.03

ÚltimaVersão:03/2024

Sumário

1.	Segurança das Informações	3
2.	Rede Corporativa	4
3.	Direitos de Acesso	4
4.	Concessão de Direitos de Acesso	4
5.	Funcionários Admitidos	5
6.	Funcionários Desligados	5
7.	Pessoal de Desenvolvimento de Sistemas	6
8.	Gerenciamento de Mudanças	6
9.	Gerenciamento de Riscos de Fornecedores	6
10.	Estações de Trabalho	6
11.	Dispositivos Móveis	7
12.	Monitoramento de Segurança	8
13.	Funções e Responsabilidade	9

1. Segurança das Informações

A GRID AGENTE AUTÔNOMO DE INVESTIMENTO LTDA (“GRID INVESTIMENTOS”) possui recurso de desenvolvimento de softwares e de suporte à própria GRID e aos usuários (TI).

A Área de Suporte e Tecnologia gerida pela empresa terceira Antrax é responsável por manter a segurança das informações disponíveis na rede corporativa da GRID INVESTIMENTOS, devendo criar condições que permitam impedir o acesso não autorizado às informações, e ao mesmo tempo manter as informações acessíveis aos usuários autorizados.

Será utilizada criptografia e implantado EFS – Encrypting File System em nosso Servidor. A criptografia será aplicada nos arquivos e pastas contido na pasta compartilhada no Servidor.

Será disponibilizado um certificado de recuperação destes arquivos, onde, somente com esse certificado combinado com uma senha conhecida apenas pelos responsáveis pela informação, se tornarão legíveis os dados do servidor caso se tornem inacessíveis via rede ou localmente.

Os sistemas de e-mail contratados devem utilizar criptografia em SMTP para envio de e-mails no aplicativo Outlook, não fazemos o uso de mídias móveis, e serão criptografadas se fizermos uso, e para backup utilizaremos o recurso de criptografia do Bucket S3 da Amazon.

Todos os sistemas operacionais e suites, estão configurados com as atualizações automáticas de segurança ativos. Os usuários não têm acesso a alteração destas configurações.

Quanto a atualizações nos equipamentos de rede compete à empresa terceirizada de TI esta avaliação, a estrutura atual é muito simples não existindo vários equipamentos na rede.

Em relação aos padrões de configurações de segurança para LANs sem fio, é utilizada a criptografia na senha WPA2.

Todas as informações enviadas serão rastreadas, sejam elas por documentos físicos através dos códigos de rastreamento dos correios, além de obter a confirmação pelo AR (Aviso de Recebimento dos Correios). Já as informações eletrônicas serão rastreáveis pelo administrador que faz o gerenciamento das contas de e-mails.

A destruição das informações também é um fator importante, todas as informações confidenciais precisam ser descartadas de forma segura. Para documentos físicos, é obrigatoriamente utilizar-se da fragmentadora de papéis. Já os documentos virtuais deverão ser repassados ao administrador que utilizará a ferramenta específica para que seja providenciado o descarte definitivo.

2. Rede Corporativa

Todos os usuários da rede corporativa da GRID INVESTIMENTOS acessam os arquivos através do servidor em nuvem Microsoft Sharepoint e são identificados através de um “login name” e uma senha do próprio Office 365. **Com o recurso do MFA (Multi Factor Authentication) imposto a todos usuários.**

Antes de acessar quaisquer recursos ou informações disponíveis na rede, o usuário deverá identificar-se através de seu login e autenticar seu acesso através de sua senha. Através de políticas de segurança, esta senha é trocada periodicamente cada 45 dias e deve atender requisitos de complexidade, conforme se segue:

Senha Padrão do Windows - Deve conter no mínimo 8 (oito) caracteres e atender, a no mínimo, a 3 (três) dos 4 (quatro) grupos de caracteres abaixo citados:

- ✓ Letras maiúsculas (de “A” a “Z”);
- ✓ Letras minúsculas (de “a” a “z”);
- ✓ Algarismos (de “0” a “9”); e
- ✓ Caracteres não-alfabéticos (Ex: “!, #, @, #, %”).

As contas padrão de usuário de sistemas, aplicações e dispositivos são imediatamente desabilitadas ou têm suas senhas trocadas antes deles serem usados em produção.

3. Direitos de Acesso

Através do sistema gerenciador de direitos de acesso (“GDA”), são concedidos ou revogados os direitos de acesso dos usuários da rede corporativa.

A revisão aos acessos lógicos é realizada periodicamente, sendo que no caso de desligamento de colaboradores a inativação ocorre de forma imediata.

4. Concessão de Direitos de Acesso

Esse sistema gerencia a concessão de direitos de acesso ao usuário utilizando o conceito de unidades de acesso, que podem ser simples ou compostas. Um exemplo de unidade de acesso simples é o acesso a um determinado diretório da rede. Um exemplo de unidade de acesso composta é o acesso a um determinado sistema, que inclui acesso a diretórios da rede, inclusão do usuário no cadastro de usuários do sistema em questão, acesso aos servidores de bancos de dados, entre outros.

O usuário faz a solicitação de acesso a uma ou mais unidades de acesso e esta é automaticamente

encaminhada pelo sistema para a aprovação de sua gerência.

Se aprovada, a solicitação é encaminhada para o setor de atendimento do Suporte, que é o centralizador das operações do GDA. Este setor analisa e, se necessário, transforma a solicitação para que esta represente a real necessidade do usuário e atenda à parametrização do sistema GDA.

Em seguida, a solicitação é encaminhada, através do GDA, para a aprovação do responsável pela unidade de acesso.

Uma vez aprovada, a solicitação é automaticamente encaminhada pelo GDA para as áreas responsáveis pela sua execução, suporte de rede, telecomunicações e desenvolvimento), que irão conceder o acesso solicitado, conforme autorizado.

Todo usuário criado deverá conter um identificador único.

5. Funcionários Admitidos

Durante o processo de admissão, e contratação de um novo funcionário ao suporte entrará em contato com o responsável da área envolvida que definirá os necessários direitos de acesso que deverão ser concedidos ao funcionário para que ele possa exercer suas funções em adequação ao seu perfil. Este processo é formalizado através do GDA.

Quando da transferência de funcionários, o gestor da área informará ao suporte e tecnologia, para que este providencie as necessárias alterações do perfil de acesso do usuário. Este processo é formalizado através do GDA.

O responsável pelo suporte realizará um levantamento de todos os recursos de informática utilizados pelo usuário na sua área de origem e informará às gerências de origem e destino do funcionário.

As gerências das áreas de origem e destino do funcionário em transferência deverão estabelecer, quais direitos de acesso deverão ser revogados, quais serão mantidos e quais deverão ser criados para que o funcionário possa executar suas novas funções. Este processo é formalizado através do GDA.

Se for necessário um período de transição, durante o qual antigos direitos de acesso precisem ser mantidos, tais direitos, bem como a duração do período de transição, devem ser especificados pelas gerências envolvidas. Após o término do período de transição os direitos de acesso serão sumariamente revogados também pelo GDA.

6. Funcionários Desligados

No caso de desligamento de funcionário, será enviado um comunicado à empresa terceirizada de TI ou

ao responsável pelo suporte, que deverá desativar o acesso do funcionário desligado à rede e ao correio eletrônico e aguardará um de acordo do GDA para revogação dos direitos deste funcionário, que deve ocorrer em até 24 horas da ocorrência do desligamento.

7. Pessoal de Desenvolvimento de Sistemas

A concessão de direitos de acesso aos responsáveis pelo desenvolvimento de sistemas também será procedida através do GDA aprovado pela gerência do desenvolvimento de sistemas e da área usuária responsável pelos dados.

8. Gerenciamento de Mudanças

Caso uma mudança seja solicitada, são reunidas informações relevantes sobre cada mudança no serviço (“por que?”, “quem pediu?”, “foi aprovado?”). O objetivo é catalogar e distribuir as medidas que devem ser tomadas ao realizar mudanças ágeis e produtivas em um projeto e, se for o caso, minimizar o impacto de eventuais incidentes.

9. Gerenciamento de Riscos de Fornecedores

Será efetuada análise prévia de novas tecnologias, serviços e produtos antes de sua contratação, com objetivo de identificar vulnerabilidade e se os fornecedores atuam de acordo com o previsto nas Políticas de PLD e PSI da GRID INVESTIMENTOS, sendo classificado seu risco e avaliada sua contratação ou não.

10. Estações de Trabalho

As estações de trabalho são protegidas através de protetores de tela (“screen savers”) os quais somente permitem o acesso mediante digitação da senha de acesso. As estações da área operacional não usam este tipo de proteção pela necessidade de estarem sempre com as informações disponíveis de forma imediata.

Após 15 minutos de ociosidade, a tela será bloqueada. Regra aplicada por GPO para todos os usuários.

As contas de Administrador das estações de trabalho têm senhas pré-definidas, totalmente desconhecidas aos usuários, ficando em posse apenas ao administrador da Empresa e ao Gestor de TI contratado.

A conta de administrador é única, para uso apenas no Server e estão sujeitas às mesmas regras das outras contas através das GPO estabelecidas a todos os usuários.

Todas as tentativas de acesso à rede malsucedidas seja de dentro das instalações da GRID

INVESTIMENTOS ou através de acesso remoto, são registradas em “log” e alertadas através de diretivas do Servidor. Após um número predeterminado de tentativas malsucedidas = 5, a conta do usuário é bloqueada e somente poderá ser desbloqueada após a intervenção de um administrador da rede, que antes de efetuar o desbloqueio analisará o problema ocorrido.

A GRID INVESTIMENTOS possui um Firewall, equipamento de prevenção de intrusões que reage de forma automática às tentativas de invasão a nossa rede a partir do mundo externo, bloqueando o ataque. Além de Software Antivírus atualizado.

No Firewall são utilizadas regras de bloqueio a listas pré-estabelecidas de sites impróprios para fins corporativos como: Sites adultos, violência, armas, hackers, drogas e outros.

Estas listas são atualizadas automaticamente, além de bloqueios aos sites de e-mails pessoais tais como Gmail, Hotmail, Yahoo, etc.

O Uso da Internet é monitorado e se houver qualquer acesso a conteúdo indevido o mesmo será bloqueado após a revisão dos acessos.

A administração de liberações e bloqueios é dinâmica e deve ser solicitada sempre através de e-mail ao responsável colaborador de TI e testada pelo solicitante após a execução da mesma.

11. Dispositivos Móveis

O colaborador da GRID INVESTIMENTOS, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na GRID INVESTIMENTOS, mesmo depois de terminado o vínculo contratual mantido com a instituição.

O dispositivo móvel de propriedade do colaborador não pode ser utilizado para fins profissionais. Caso haja necessidade de utilização de dispositivo móvel para fins profissionais, o seu fornecimento deve ser aprovado pela GRID INVESTIMENTOS.

Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados do dispositivo móvel. Deverá, também, manter estes backups separados do dispositivo móvel, ou seja, não os carregar juntos. Há a disponibilidade técnica de se implantar esses backups em nuvem e deve ser considerada pelo colaborador.

O suporte técnico aos dispositivos móveis eventualmente fornecidos pela GRID INVESTIMENTOS a seus colaboradores deverá seguir o mesmo fluxo do suporte contratado pela instituição para os demais serviços relacionados a tecnologia da informação.

Todo colaborador deverá utilizar senhas de bloqueio automático para o dispositivo móvel.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico autorizado.

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico autorizado.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

Os dispositivos móveis atuam em rede separada por roteador, não há acesso à rede e todos os dispositivos com acesso à rede possuem antivírus instalado.

É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel, notificar imediatamente seu gestor direto e ao responsável por sistemas. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à GRID INVESTIMENTOS e/ou a terceiros.

12. Monitoramento de Segurança

Outra proteção é o Firewall que registra todos os eventos suspeitos relacionados ao acesso à rede corporativa através da Internet e disponibiliza aos administradores um relatório com um resumo das ocorrências por período pré-determinado. De posse deste relatório, os eventos são analisados caso a caso e as devidas providências são tomadas.

Os antivírus têm um mecanismo inteligente e automático sob a forma de quarentena de remoção de vírus ou arquivos suspeitos de infecção, qualquer bloqueio incorreto deve ser solicitado a equipe técnica sob o conhecimento do responsável.

A Administração é remota e via Cloud, qualquer suspeita ou anormalidade no comportamento da máquina deve ser imediatamente comunicada a equipe técnica.

13. Funções e Responsabilidade

A Política deverá ser atualizada pelo menos uma vez ao ano, em revisões programadas, ou toda vez que uma mudança considerável ocorra nos serviços críticos executados pelo processo de negócio (ex. número de colaboradores, mudança para outra localidade etc.). Todo colaborador ao ingressar na GRID INVESTIMENTOS deverá ler essa Política e registrar seu entendimento e conhecimento em Termo de Ciência e Compromisso.

Para todos os prestadores de serviços contratados é necessária uma diligência antes da contratação, analisando sua experiência através do tempo de existência, clientes, qualidade do serviço prestado e verificação dos antecedentes criminais.

Para todos os contratos firmados é necessário que conste previamente uma cláusula de confidencialidade entre os prestadores de serviços, assegurando assim a segurança das informações.

Ciclos de treinamentos sobre esta Política serão realizados anualmente. Os assuntos incluirão phishing, confidencialidade da informação, ética voltada aos conceitos e processos de TI, o que inclui o uso apropriado das senhas, bem como das informações corporativas.

Ações de melhoria para esta Política serão registradas e gerenciadas sempre que a mesma receber algum retorno ou sugestão, ou ainda quando avaliar os aprendizados e a evolução dos processos e da tecnologia.