1. Objetivo do documento

A Política de Segurança da Informação tem como objetivo estabelecer normas, diretrizes e procedimentos que assegurem a segurança das informações, ao tempo que não impeçam e/ou dificultem o processo do negócio, mas que garantam:

- A confiabilidade das informações através da preservação da confidencialidade, integridade e disponibilidade dos ativos da empresa;
- O compromisso da empresa com a proteção das informações de sua propriedade e/ou sob sua guarda;
- A participação e cumprimento por todos os colaboradores em todo o processo.

2. Abrangência da aplicação do documento

Aplica-se a todos os departamentos do Grupo GRECA, que abrange as empresas AJG PARTICIPACOES SOCIETARIAS LTDA., ARTHUR GRECA SCHMUCK CONSULTORIA EMPRESARIAL, ATRIA S/A - CREDITO, FINANCIAMENTO E INVESTIMENTO, BRASIL MINERACAO E TRANSPORTES LTDA., GRCA PARTICIPACOES LTDA, GREGOR PARTICIPACOES LTDA, MAJIC PARTICIPACOES S/A, MAJIC II PARTICIPACOES S/A, GRECA DISTRIBUIDORA DE ASFALTOS LTDA., GRECA TRANSPORTES DE CARGAS LTDA.

3. Responsabilidades

3.1 Colaboradores

Será de inteira responsabilidade dos colaboradores das empresas do Grupo GRECA:

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação do Grupo GRECA;
- Buscar o departamento de Tecnologia da Informação para esclarecimentos de dúvidas referentes à Política de Segurança da Informação, bem como ter entendimento sobre o procedimento interno “TI-P001 - Governança de Tecnologia da Informação”, que define as diretrizes básicas da administração da Tecnologia da Informação para a segurança, manutenção e evolução da estrutura e dos serviços oferecidos e suportados pelo setor;
- Proteger as informações contra acesso, divulgação, modificação ou destruição não autorizados pelo Grupo GRECA;
- Garantir que equipamentos e recursos tecnológicos à sua disposição sejam utilizados apenas para finalidades profissionais e devidamente aprovadas;
- Descarte adequado de documentos de acordo com seu grau de classificação;
- Comunicar prontamente à chefia imediata qualquer violação a esta política, suas normas e procedimentos.

3.2 Gestores

Em relação à Segurança da Informação, cabe aos coordenadores, supervisores, gerentes e diretores:

- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob sua gestão;
- Dar ciência, na fase de contratação e formalização dos contratos individuais de trabalho, à responsabilidade do cumprimento da PSI no Grupo GRECA;
- Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação;
- Exigir de parceiros, prestadores de serviço e outras entidades externas, a assinatura do termo de confidencialidade referente às informações às quais terão acesso;
- Elaborar, com apoio do departamento de Tecnologia da Informação, os procedimentos de segurança da informação relacionados às suas áreas, fornecendo as informações necessárias e mantendo-os atualizados;
- Informar, sempre que necessário, atualizações referentes a processos e/ou cadastros de funcionários para que as permissões possam ser concedidas ou revogadas de acordo com a necessidade.

3.3 Comitê de Segurança da Informação

Cabe ao Comitê de Segurança da Informação:

- Aprovar a Política de Segurança da Informação e suas atualizações;
- Propor melhorias, alterações e ajustes da PSI;
- Propor investimentos relacionados à segurança da informação com o intuito de minimizar os riscos;
- Classificar e reclassificar o nível de acesso às informações sempre que necessário;
- Avaliar ocorrências de segurança e propor ações corretivas;
- O Comitê de Segurança da Informação deverá ser composto por, no mínimo, um colaborador dos seguintes departamentos:
    - Diretoria Administrativa;
    - Tecnologia da Informação;
    - Jurídico;
    - Recursos Humanos;
    - Atria Financeira;
    - Controles Internos.
- O Comitê de Segurança da Informação se reunirá uma vez a cada seis meses e extraordinariamente sempre que for necessário deliberar sobre alguma ocorrência grave ou definição relevante para o Grupo GRECA.

3.4 Departamento de Tecnologia da Informação

Cabe ao Departamento de Tecnologia da Informação:

- Definir as regras para instalação de software e hardware no Grupo GRECA;
- Monitorar os acessos às informações e aos ativos de tecnologia (sistemas, banco de dados, recursos de rede), tendo como referência a Política e as Normas de Segurança da Informação;
- Manter registro e controle atualizados de todas as liberações de acesso concedidas, providenciando, sempre que demandado formalmente, a pronta suspensão ou alteração de tais liberações;
- Propor as metodologias e processos referentes à segurança da informação, como classificação da informação, avaliação de risco, análise de vulnerabilidade etc.;
- Promover palestras e comunicados de conscientização dos colaboradores em relação à importância da segurança da informação para o negócio do grupo;
- Analisar criticamente ocorrências de segurança em conjunto com o Comitê de Segurança da Informação;
- Buscar alinhamento com as diretrizes do grupo;
- Possibilitar e facilitar a auditoria nos ativos sob sua responsabilidade, seja através de módulos de auditoria no desenvolvimento de sistemas, na escolha de contratação de serviços que permitam auditabilidade, ou na disponibilização dos registros de um ativo, quando existir.

4. Distribuição e vigência

Este documento consiste na Política de Segurança da Informação (PSI) do Grupo GRECA, que deve ser mantida como uma medida de boas práticas, estabelecendo diretrizes para a prevenção e proteção de ativos, bem como definição de responsabilidades. Destaca-se que a mesma deve ser adotada, cumprida e aplicada em todas as áreas da empresa.

Esta versão pode ser alterada a qualquer momento, uma vez que os pontos identificados para mudanças sejam informados e discutidos com os demais colaboradores da mesma. Contudo, a versão da PSI deve ser revisada a cada ano, considerando a data de sua aprovação.

Em havendo atualizações, essas serão divulgadas a todos os colaboradores.

5. Glossário

- Ativo: Algo que tenha valor para a organização;
- Evento: Acontecimento que acarrete na mudança do estado atual do processo;
- Ocorrência: Incidente que traz prejuízos à empresa;
- Risco: Combinação da probabilidade de ocorrência de um evento e seus respectivos impactos;
- Vulnerabilidade: Fragilidade de um ativo que pode ser explorada e gerar danos à organização;
- Malwares: Qualquer tipo de programa indesejado, instalado sem seu consentimento e que pode trazer danos ao computador;

- SPAM: É o termo usado para referir-se a e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;
- *Phishing*: Mensagens de e-mail que solicitam dados do usuário de forma direta ou através do redirecionamento para sites ou números de telefones, a fim de roubar sua identidade;
- *Mail bombing*: Envio de mensagens eletrônicas em massa para um determinado destinatário com o objetivo de sobrecarregar o serviço de e-mail e torná-lo inutilizável ou indisponível;
- *Multifator de autenticação*: método de autenticação que requer mais de uma forma de identificar e verificar a identidade de um usuário.

6. Descrição da Política

6.1 Introdução

A presente Política de Segurança da Informação (PSI) está baseada nas recomendações da norma ABNT NBR isso/IEC 27002:2013, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, e também em conformidade com a Resolução nº 4.893 de 26 de fevereiro de 2021 do Banco Central do Brasil, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

A informação é um ativo de grande valor para o Grupo GRECA, por isso necessita ser adequadamente protegida.

Por princípio, a Segurança da Informação deve abranger três propriedades básicas:

- Confidencialidade: Informações devem estar acessíveis apenas para pessoas autorizadas;
- Integridade: Informações não devem sofrer alterações durante o seu processamento;
- Disponibilidade: Informações devem estar sempre acessíveis, a qualquer momento, para uso legítimo de pessoas autorizadas.

6.2 Por que os colaboradores devem se preocupar com segurança?

De nada adianta a área de Tecnologia da Informação impor controles e medidas técnicas se não existir a participação dos colaboradores. A TI pode implementar barreiras e portas de controle de acesso eletrônico, mas se um funcionário que tem acesso legítimo a determinada área restrita resolve divulgar informações confidenciais que estavam devidamente protegidas nesta área, todo esforço é em vão.

A área de Tecnologia da Informação é a responsável pela salvaguarda dos dados da organização, mas o processo de segurança da informação deve envolver todos os colaboradores, independentemente do nível hierárquico, posto que, de posse de uma informação específica, qualquer pessoa pode, por descuido ou com má intenção, se tornar um agente de divulgação não autorizada.

Diante do exposto, a Política de Segurança da Informação vem propor uma Gestão de Segurança da Informação baseada em controles e procedimentos técnicos, considerando e promovendo o comportamento dos colaboradores de forma que possa aplicar a tecnologia adequada em todo o processo e atingir efetivamente seu objetivo: entender o negócio e aplicar segurança a ele.

6.2.1 Educação e conscientização sobre as práticas de Segurança da Informação adotadas pelo Grupo

A TI do Grupo GRECA conduz treinamentos periódicos de conscientização como medidas de prevenção e redução de riscos, de forma a nivelar o conhecimento entre os usuários e manter um comportamento seguro com relação à informação.

Também são realizadas campanhas através de e-mail, bem como divulgação de material educativo em mural informativo.

6.3 Alta direção

A efetividade da Política de Segurança da Informação depende estritamente do comprometimento da alta direção. É essencial que os responsáveis por liberar recursos, aplicar sanções e criar regras apoiem a PSI e demonstrem seu comprometimento para que os colaboradores se sintam motivados a cumpri-la. Dessa forma, a alta direção do Grupo apresenta seu compromisso com a melhoria contínua dos procedimentos relacionados à PSI.

A ordem expressa e o exemplo de cumprimento das cláusulas da PSI pela alta direção possibilitarão:

- A inexistência de exceções à regra;
- Que a PSI seja um ativo estratégico;
- Que a PSI tenha ampla divulgação;
- Que a PSI seja incluída no processo de contratação de novos funcionários.

Caso essas premissas não sejam cumpridas, a Política de Segurança da Informação se tornará apenas um documento obsoleto, existente na teoria e não adotado na prática.

6.4 Classificação e manuseio das informações

As informações são classificadas e identificadas considerando os seguintes níveis:

- Pública: São informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não compromete o negócio e que, por isso, não necessitam de proteção efetiva ou tratamento específico.
  São exemplos de informações públicas:
  - Editais de licitação;
  - Catálogo de serviços.

- Interna: São informações disponíveis aos colaboradores do Grupo GRECA para a execução de suas tarefas rotineiras, não se destinando, portanto, ao uso do público externo.
  São exemplos de informações internas:
  - Memorandos, padrões, políticas e procedimentos internos;
  - E-mails e ramais internos;
  - Avisos e campanhas internas.

- Confidencial: São informações de acesso restrito a um colaborador ou grupo de colaboradores. Sua revelação pode violar a privacidade de indivíduos, violar os acordos de confidencialidade, dentre outros.
  São exemplos de informações confidenciais:
  - Processos judiciais;
  - Dados cadastrais de funcionários;
  - Dados contábeis.

- Confidencial restrito: São informações de acesso restrito a um colaborador ou grupo de colaboradores que obrigatoriamente contam como destinatários da mesma, em geral, associadas ao interesse estratégico da empresa e restritas a diretores, gerentes e funcionários cujas funções requeir6ropboxecê-las.
  São exemplos de informações confidenciais restritas:
  - Atas de reunião da diretoria;
  - Indicadores e estatísticas dos processos de negócio do grupo;
  - Resultado de auditorias internas.

O manuseio das informações pertencentes ao Grupo GRECA deve levar em consideração as regras de sigilo acima estipuladas, conforme explicitado na política interna de TI "TI-P0–3 - Processo de Armazenamento e Manuseio Eletrônico de Arquivos".

6.5 Utilização da Rede e Internet

O ingresso à rede corporativa do Grupo GRECA deve ser devidamente controlado conforme definido no procedimento interno da TI "TI-P0–9 - Procedimento para Conexão de Equipamentos à Rede" para que os riscos de acessos sejam minimizados. Assim, é preciso que sejam respeitadas algumas regras, listadas a seguir:

1. O acesso à rede corporativa (Greca Corporativo), tanto cabeada quanto por rede sem fio, estará disponível apenas para máquinas e equipamentos do Grupo GRECA, com a finalidade restrita à realização de atividades inerentes à função que desempenha;
2. Para eventuais acessos de terceiro à rede corporativa, o departamento responsável pelo visitante deverá preencher o formulário interno da TI "TI-F0–9 - Acesso de visitante ao ambiente Greca Corporativo", informando a justificativa, período que o visitante estará na empresa, e obter as devidas aprovações para viabilizar a liberação. Além disso, o terceiro deverá estar ciente da Política de Segurança para Terceiros;

3. A concessão de acesso à rede sem fio para visitantes (GRECA Visitante) para acesso à Internet se dará através de solicitação do requisitante –por um *voucher* de acesso, o qual dará direito de acesso por tempo limitado mediante cadastro;
4. O departamento de Recursos Humanos ficará responsável por notificar formalmente o departamento de TI sobre desligamentos ou mudança de área de colaboradores, para que os acessos dos mesmos sejam revogados;
5. O departamento de TI reserva-se o direito de monitorar e registrar o acesso à Internet como forma de inibir a proliferação de programas maliciosos, garantindo a integridade da rede, sistemas e dados internos;
6. Os equipamentos, tecnologias e serviços fornecidos para o acesso à Internet são de propriedade do departamento de TI, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação, visando assegurar o cumprimento de sua Política de Segurança da Informação;
7. É proibida a divulgação e/ou o compartilhamento indevido de informações internas, confidenciais e restritas em listas de discussão, sites, redes sociais, fóruns, comunicadores instantâneos ou qualquer outra tecnologia correlata que use a internet como via, de forma deliberada ou inadvertidamente, sob a possibilidade de sofrer penalidades previstas nos procedimentos internos e/ou na forma da lei;
8. Os colaboradores com acesso à Internet não poderão realizar download de programas. Estes, se estiverem alinhados às necessidades da atividade, deverão ser solicitadas ao departamento de TI, que deverá providenciar a instalação, licenciamento e os devidos registros, se necessário;
9. O nível de acesso à internet concedido ao colaborador deverá ser definido e formalizado pelo seu gestor, conforme especificado no procedimento de TI “TI-P0–9 - Gestão de Acessos à Internet”;
10. O uso, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente são expressamente proibidos. Qualquer software não autorizado será excluído pelo departamento de TI, e as devidas sanções poderão ser aplicadas;
11. Os colaboradores não poderão em hipótese alguma utilizar os recursos de tecnologia da informação do Grupo GRECA para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional;
12. Como regra geral, materiais de cunho sexual ou que ofendam as leis, moral e os bons costumes não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso, conforme detalhado no procedimento interno de TI “TI-P0–0 - Procedimento para Disponibilização de Uso e Recursos de TI”;
13. Documentos digitais de condutas consideradas ilícitas, como por exemplo apologia ao tráfico de drogas e pedofilia, são expressamente proibidos e não devem ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;
14. Os colaboradores não poderão usar os recursos para deliberada ou inadvertidamente propagar qualquer tipo de vírus ou programas maliciosos, conforme detalhado no procedimento interno de TI “TI-P0–8 - Procedimento de Medidas Preventivas contra Vírus”;

15. Não serão permitidos os acessos a softwares *peer-to-peer* (Kazaa, BitTorrent e afins);
16. Não serão permitidos os acessos a sites de compartilhamento de arquivos, tais como: mega, upload, bitshare, depositfile8ropboxbox, wetransfer etc.;
17. Não serão permitidas tentativas de burlar os controles de acesso à rede, tais como utilização de proxies anônimos e estratégias de by-pass de firewall;
18. Não serão permitidos o uso de aplicativos de reconhecimento de vulnerabilidades, análise de tráfego, ou qualquer outro que possa causar sobrecarga ou prejudicar o bom funcionamento e a segurança da rede interna, salvo os casos em que o objetivo for realizar auditorias de segurança quando o departamento de TI deverá estar devidamente ciente e concedido autorização para tal;
19. Os arquivos inerentes ao Grupo GRECA, obrigatoriamente, deverão ser armazenados na pasta compartilhada de cada setor, localizada no servidor de arquivos conforme detalhado nos procedimentos interno de TI "TI-P0–3 - Processo de Armazenamento e Manuseio Eletrônico de Arquivos" e "TI-P0–7 - Procedimento para Backup e Restore", para a garantia de backup destes documentos. É terminantemente proibido armazenar estes tipos de arquivos em equipamentos pessoais;
20. A manipulação dos arquivos deve seguir a política de confidencialidade definida para o Grupo, conforme detalhado no procedimento interno de TI "TI-P0–3 - Processo de Armazenamento e Manuseio Eletrônico de Arquivos";
21. Não será permitida a alteração das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro;
22. Haverá geração de relatórios de sites e downloads acessados por usuários;
23. O uso recreativo poderá ser autorizado em horário de almoço, entre às 12:00 e 13:15, com tolerância de 15 minutos, de forma controlada, visando o não comprometimento de performance da rede interna do Grupo GRECA e da internet, cumprindo todas as demais regras presentes nesta política.

6.6 Política de Senhas

A senha é a forma mais convencional de identificação de acesso do usuário. É um recurso pessoal e intransferível que protege a identidade do colaborador, evitando que uma pessoa se faça passar por outra, conforme definido em procedimento interno de TI "TI-P0–7 - Gestão de Acessos de TI".

O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Assim, com o objetivo de orientar a criação de senhas seguras e a devida proteção, estabelecem-se as seguintes regras:

1. A senha é de total responsabilidade do colaborador, sendo expressamente proibida sua divulgação ou empréstimo, devendo a mesma ser imediatamente alterada no caso de suspeita de vazamento;

2. A senha inicial só será fornecida ao próprio colaborador, pessoalmente. Não poderão ser fornecidas por telefone, comunicador instantâneo ou qualquer outra forma que não assegure a identidade do colaborador;
3. O gestor direto do colaborador pode intermediar a entrega da primeira senha, no momento do primeiro acesso, e esta deve ser alterada imediatamente;
4. É proibido o compartilhamento de login para funções de administração de sistemas;
5. As senhas não devem ser anotadas e deixadas próximo ao computador (debaixo do teclado, colada no monitor etc.);
6. As senhas deverão seguir os seguintes pré-requisitos:
    a. Tamanho mínimo de dez caracteres;
    b. Deve ser composta por uma mistura de letras (maiúsculas e minúsculas), números e caracteres especiais;
    c. Não devem ser baseadas em informações pessoais de fácil dedução (aniversário, nome do cônjuge etc.);
    d. Não é permitido o uso de uma senha idêntica às cinco mais recentes para o mesmo usuário.
7. O acesso do usuário deverá ser imediatamente revogado nas seguintes situações:
    a. Desligamento do colaborador;
    b. Mudança de função do colaborador;
    c. Quando, por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação.
8. A senha é bloqueada após cinco tentativas malsucedidas de login. Somente a TI pode desbloquear, caso o sistema não possua o processo “recuperar senha”;
9. Para os cancelamentos acima mencionados, o departamento de Recursos Humanos ficará responsável por informar prontamente o departamento de Tecnologia da Informação acerca dos desligamentos e mudança de função dos colaboradores;
10. Sempre que disponível, o multifator de autenticação deverá ser utilizado em contas corporativas.

6.7 E-mail

O e-mail é uma das principais formas de comunicação. No entanto, é também uma das principais vias de disseminação de malwares, por isso, surge a necessidade de normatização da utilização deste recurso, conforme orientado no procedimento interno de TI “TI-P0–0 - Procedimento para Disponibilização de Uso e Recursos de TI”. Abaixo regras de utilização:

1. O e-mail corporativo é destinado a fins profissionais, relacionados às atividades dos colaboradores;
2. Os e-mails enviados ou recebidos de endereços externos poderão ser monitorados com o intuito de bloquear spams, malwares ou outros conteúdos maliciosos que violem a Política de Segurança da Informação;

3. É proibido enviar, com endereço eletrônico corporativo, mensagens com anúncios particulares, propagandas, vídeos, fotografias, músicas, mensagens do tipo “corrente”, campanhas ou promoções;
4. É proibido abrir arquivos com origens desconhecidas anexados a mensagens eletrônicas;
5. É proibido enviar qualquer mensagem por meios eletrônicos que torne o Grupo GRECA vulnerável a ações civis ou criminais;
6. É proibido falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;
7. É proibido produzir, transmitir ou divulgar mensagem que:
    a. Contenha ameaças eletrônicas, como: spam, phishing, mail bombing, malwares;
    b. Contenha arquivos com código executável (.exe, .cmd, .pif, .js, .hta, .src, cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
    c. Vise obter acesso não autorizado a outro computador, servidor, sistema ou rede;
    d. Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
    e. Vise burlar qualquer sistema de segurança;
    f. Vise vigiar secretamente ou assediar outro usuário;
    g. Vise acessar informações confidenciais sem explícita autorização do proprietário;
    h. Tenha conteúdo considerado impróprio, obsceno ou ilegal;
    i. Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
    j. Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.
8. O uso de e-mails para fins pessoais é proibido;
9. Para garantia da segurança e identificação do indivíduo, a autenticação em dois fatores é habilitada para login e recuperação de senha, através do envio de uma mensagem de texto para o telefone pessoal do colaborador, cujo número deverá ser informado à TI para disponibilizar o serviço, ou através de aplicativo autenticador instalado no celular pessoal ou corporativo do colaborador.

6.8 Uso das Estações de Trabalho

As estações de trabalho devem permanecer operáveis durante o maior tempo possível para que os colaboradores não tenham suas atividades prejudicadas, e devem ser utilizados conforme definido no procedimento interno da TI, "TI-P010 - Procedimento para Disponibilização de Uso e Recursos de TI". Assim, algumas medidas de segurança devem ser tomadas, são elas:

1. É de responsabilidade do colaborador zelar pelo seu computador e periféricos, mantendo-os em boas condições;
2. Não é permitido personalizar o equipamento por adesivos, fotos, riscos, raspar e retirar etiquetas;

3. É vedada a abertura de computadores para qualquer tipo de reparo pelos colaboradores. Caso seja necessário, o reparo deverá ser feito pela equipe do departamento de TI ou profissionais autorizados pela TI;
4. As estações de trabalho só estarão acessíveis aos colaboradores através de contas de usuário limitadas
5. É proibida a instalação de softwares ou sistemas nas estações de trabalho pelos usuários finais. Este procedimento só poderá ser realizado pela equipe do departamento de TI;
6. É proibida a instalação de softwares que não possuam licença e/ou não sejam homologados pela equipe do departamento de TI;
7. As estações de trabalho devem permanecer bloqueadas nos períodos de ausência do colaborador;
8. Os documentos e arquivos relativos à atividade desempenhada pelo colaborador deverão, sempre que possível, serem armazenados em local próprio no servidor da rede, o qual possui rotinas de backup e controle de acesso adequado;
9. Documentos críticos e/ou confidenciais só podem ser armazenados no servidor da rede, nunca na unidade de armazenamento local da máquina;
10. É proibido o uso de estações de trabalho para:
    a. Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
    b. Burlar quaisquer sistemas de segurança;
    c. Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
    d. Cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
    e. Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
11. O departamento de TI não se responsabiliza por prestar manutenção ou instalar softwares em computadores que não sejam os da empresa;
12. As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário.

6.9 Uso de Equipamentos Particulares

A utilização de equipamentos particulares na rede corporativa (Greca Corporativo) do grupo não é permitida. Entretanto havendo justificativa pertinente, a TI pode flexibilizar a utilização, mitigando os riscos através de algumas regras, conforme segue:

1. Fica autorizado o uso de notebooks para acesso à rede interna do Grupo GRECA mediante autorização do gestor imediato, com as devidas justificativa e formalização da solicitação conforme procedimento interno de TI, "TI-P002 - Gestão de Serviços";
2. O departamento de TI deverá verificar as configurações de rede, do aplicativo de antivírus e demais aplicativos instalados para que o acesso à rede interna seja concedido. Caso o

equipamento não obedeça aos requisitos mínimos de segurança, o acesso não será concedido;

3. O departamento de TI tem o direito de, periodicamente, auditar os equipamentos utilizados no Grupo GRECA, visando proteger suas informações bem como garantir que aplicativos ilegais não estejam sendo usados na infraestrutura da empresa;
4. É de responsabilidade do proprietário a instalação do Sistema Operacional que será utilizado, bem como dos aplicativos a serem utilizados no notebook, salvo exceções de aplicativos específicos autorizados pelo departamento de TI;
5. É de responsabilidade do proprietário usar somente aplicativos legalizados em seu notebook;
6. Não podem ser executados nos notebooks aplicativos de característica maliciosa, que visam comprometer o funcionamento da rede, acesso a informações sem a devida permissão ou informações confidenciais;
7. É proibido o armazenamento de informações que não sejam de uso pessoal do proprietário do computador pessoal. Todos os arquivos que pertençam ao Grupo GRECA não podem ser armazenados no disco rígido do notebook ou em dispositivos de armazenamento móvel (ex: pendrive), sem a autorização da área responsável pelos dados. Estes arquivos devem sempre ser armazenados no servidor de compartilhamento destinado para tal;
8. Mesmo nos computadores portáteis fornecidos pelo Grupo GRECA, é proibido o armazenamento de informações confidenciais e confidenciais restritas no disco rígido do equipamento;
9. É proibida a inclusão de smartphones na rede corporativa do Grupo GRECA. Quando autorizado, estes equipamentos deverão ter seu acesso restrito à rede visitante;
10. Quaisquer danos causados, físico ou lógico, pelo computador pessoal ou através deste será de responsabilidade do proprietário do computador;
11. O Grupo GRECA não se responsabiliza por quaisquer danos causados ao computador pessoal, sejam físicos ou lógicos;
12. O departamento de TI reserva o direito de negar ou revogar a utilização de um computador pessoal no ambiente e rede corporativos a qualquer momento.

6.10 Uso de Impressoras e Scanners

O uso de impressoras e scanners no Grupo GRECA deve seguir algumas regras:

- É proibida a impressão e cópia de documentos de cunho pessoal e/ou ilegal;
- A configuração e manutenção das impressoras só podem ser realizadas pela equipe do departamento de TI ou empresa terceira contratada, exceto a troca de toner, que pode ser realizada pelo departamento/unidade, lembrando de sempre reportar à TI;
- O gestor de cada departamento/unidade será o responsável pela impressora localizada na sala, inclusive para responder a questionamentos como impressões/cópias excessivas;
- O escaneamento de arquivos pessoais nas multifuncionais do Grupo é proibido;
- É proibido o envio de documentos escaneados diretamente da multifuncional para domínios de empresas que não sejam do Grupo GRECA.

6.11 Backup

Um dos procedimentos mais básicos da Segurança da Informação é a implantação de uma Política de Backup (cópia de segurança). Uma organização tem que estar preparada para recuperar (restaurar) todos os seus dados de forma íntegra caso uma ocorrência de perda de dados venha a ocorrer. O Grupo GRECA possui essa política estabelecida, conforme formalizado no procedimento interno de TI, "TI-P027 - Procedimento para Backup e Restore". Assim, estabelecem-se as regras:

1. Todo sistema ou informação relevante para a operação dos negócios do Grupo GRECA deve possuir cópia dos seus dados de produção para que, em eventual ocorrência de indisponibilidade de dados, seja possível recuperar ou minimizar os impactos nas operações do grupo;
2. As áreas de negócio ficarão responsáveis por classificar os dados de acordo com a relevância e provocar o departamento de TI sobre a necessidade de backup dos mesmos, sugerindo o tempo de retenção destas cópias;
3. Todos os backups devem ser automatizados por sistemas de agendamento para que sejam, preferencialmente, executados fora do horário comercial, períodos de pouco ou nenhum acesso de usuários ou processos aos sistemas de informática;
4. As mídias de backup devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e, preferencialmente, distantes o máximo possível do data center;
5. Toda infraestrutura de suporte aos processos de backup e restauração deve possuir controles de segurança para prevenção contra acessos não autorizados, bem como mecanismos que assegurem seu correto funcionamento;
6. O departamento de TI deve preparar semestralmente um plano para execução de testes de restauração de dados, que deve ter escopo definido em conjunto com as áreas de negócio. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos;
7. Na situação de erro de backup e/ou restauração é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema. Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser executados apenas mediante justificativa de necessidade.

6.12 Perda, Roubo ou Dano a Recursos de TI

Em caso de perda, roubo ou dano a recursos de TI, deverá ser realizado o registro da ocorrência para o setor de TI para sua devida tratativa.

O valor de conserto por mau uso, reposição ou extravio do dispositivo será debitado no centro de custo do colaborador, que poderá sofrer o desconto referente ao valor, nos termos da lei e do contrato de trabalho mantido pelas empresas do Grupo GRECA.

Os detalhes desse procedimento estão disponíveis em "TI-P020 - Procedimento para Perda, Roubo ou Dano a Recursos de TI".

6.13 Segurança do Ambiente de TI

6.13.1 Estrutura Física do Data Center

A restrição de acesso físico ao data center pretende promover proteção aos ativos de TI, garantindo a salvaguarda dos dados nele contido, tão quanto a preservação da correta execução dos sistemas e ambientes corporativos. Esse controle está previsto em procedimento interno da TI, conforme "TI-P026 - Segurança Física do Data Center". Desta forma, define-se nesta política que:

1. As máquinas (servidores) que armazenam sistemas e dados do Grupo GRECA estão em área protegida, dentro do data center localizado na sala do departamento de TI, na Matriz do grupo, em Araucária.
2. Todos os sistemas ou equipamentos classificados como críticos devem ser mantidos em áreas seguras do data center;
3. A entrada ao data center tem acesso devidamente controlado e monitorado. As permissões de acesso físico às áreas restritas do data center devem ser mensalmente revisadas;
4. As áreas do data center devem ser protegidas com barreiras de segurança ou mecanismos de acesso, de forma a impedir o acesso não autorizado;
5. A porta do data center deve permanecer fechada, com mecanismo de autenticação individual quando possível;
6. O acesso às dependências do data center com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só pode ser feito a partir de autorização da equipe de TI e mediante supervisão;
7. O acesso ao data center sem as devidas identificações só poderá ocorrer em situações de emergência, quando a segurança física do data center for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação não estiver funcionando;
8. Caso haja necessidade do acesso não emergencial, o requisitante deve solicitar autorização com antecedência a qualquer colaborador responsável pela administração de liberação de acesso;
9. O data center deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do departamento administrativo;
10. Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

6.13.2 Estrutura Lógica do Data Center

Na Política de Segurança da Informação estabelecida pelo Grupo GRECA, define-se que os analistas de TI, mediante ciência do Comitê de Segurança da Informação, devem ser os únicos a terem permissão para ler/editar as informações, obedecendo as atribuições de sua área de atuação.

O objetivo da segurança lógica no data center é proteger os ativos de informações, sistemas ou programas de acesso indevidos e não autorizados.

Somente os colaboradores credenciados e autorizados pelo Comitê de Segurança da Informação podem ter acesso aos dados armazenados.

Os logs dos ativos de rede devem ser monitorados constantemente a fim de evitar acessos indevidos.

6.14 Incidentes e Ocorrências de TI

Um incidente é a interrupção não planejada de um serviço de TI ou a redução da qualidade do serviço prestado. Essa definição é dada pelo ITIL, uma biblioteca de boas práticas em gerenciamento de serviços de TI (ITSM).

São exemplos de incidentes: falta de acesso à internet, servidor fora do ar, mau funcionamento de computadores etc. Eles podem ser identificados pela equipe de TI, por sistemas de monitoramento ou, então, relatados pelos usuários e clientes.

Esses incidentes são tratados pelo departamento de TI do Grupo GRECA conforme procedimento interno da TI, "TI-P002 - Gestão de Serviços".

Caso o incidente em questão tenha ocasionado algo de maior gravidade, é aberta uma ocorrência de TI, que visa comunicar, todos os departamentos impactados, identificar causa raiz, definir responsabilidades, plano de ação e acompanhamento até a solução final, a fim de eliminar a possibilidade da recorrência. Esse processo está definido conforme procedimento interno de TI, "TI-P032 - Procedimento para Reporte de Ocorrências de TI".

Quaisquer falhas, anomalias, ameaças ou vulnerabilidades observadas devem ser notificadas o mais rápido possível através do e-mail: suporte@grecaasfaltos.com.br, que resultará na abertura de chamado para TI.

6.14.1 Gestão de Riscos

O gerenciamento de riscos é uma das bases da governança e visa garantir que, caso ocorra alguma falha em quaisquer das operações, esta não coloque em risco os objetivos estratégicos da empresa, uma vez que os riscos relacionados às operações podem ter impactos no sucesso da corporação.

O processo de inclusão e revisão é contínuo, e tão logo novos riscos são identificados, a diretoria é envolvida a fim de decidir a estratégia e ações a serem adotadas para a tratativa dos riscos.

O procedimento conduzido pela TI encontra-se detalhado em "TI-P030 - Gestão de Riscos de TI".

6.15 Continuidade do Negócio em Situações de Crise

As situações de crise são caracterizadas pela ocorrência de incidentes relevantes em ativos críticos de tecnologia da informação que possam interromper e comprometer a operação das filiais, matriz, ou todas as empresas do Grupo. Também são consideradas situações de crise, desastres ou falhas relacionadas a invasão ou vazamento de dados de clientes, fornecedores, colaboradores e prestadores de serviços.

Configuram situações de crise:

- Desastres que provoquem a inoperância do data center por mais de 96 horas;
- Invasões cibernéticas que paralisem as atividades do grupo;
- Sequestro ou vazamento de dados de clientes, fornecedores, colaboradores e prestadores de serviços.

Em caso de crise, um plano está definido e configurado para contemplar ações de contorno ou ativação de infraestrutura de contingência local ou, em conjunto com a comunicação tempestiva do incidente relevante ao Banco Central, para que as cargas de trabalho da empresa possam ser recuperadas e disponibilizadas imediatamente, mitigando desta forma danos à operação.

Detalhes desse processo podem ser encontrados nos procedimentos internos de TI "TI-P024 - Plano de Contingência de TI" e "TI-P025 - Procedimento de Acionamento de Disaster Recovery".

6.16 Contratação de serviços em nuvem

Em caso de necessidade de contratação de serviços em nuvem, deverão ser considerados a relevância do serviço a ser contratado, a criticidade do serviço e a sensibilidade dos dados que serão manipulados pelo fornecedor. Quanto mais sensível os dados manipulados, mais cuidado deverá ser tomado.

Desta forma, deverão estar assegurados pontos como:

- Cumprimento da legislação e da regulamentação em vigor, incluindo a Resolução nº 4.893 de 26 de fevereiro de 2021 do Banco Central do Brasil, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de processamento e armazenamento de dados e de computação e nuvem;
- Acesso da instituição contratante aos dados processados ou armazenados pelo prestador de serviço;
- Confidencialidade, a integridade, a disponibilidade e a recuperação dos dados processados ou armazenados pelo prestador de serviço;
- Provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados, incluindo relatórios de auditoria independente;
- Identificação e segregação dos dados dos clientes da instituição por meio de controles físicos e/ou lógicos;
- Qualidade dos controles de acesso voltados à proteção dos dados dos clientes da instituição.

Os detalhes podem ser encontrados no procedimento "TI-P033 - Procedimento para Contratação de Serviço em Nuvem".

6.17 Informações ao Banco Central do Brasil

Em atendimento ao art. 23º da Resolução 4.893, devem ficar à disposição do Banco Central do Brasil pelo prazo de cinco anos:

1. A Política de Segurança da Informação do Grupo;
2. O documento relativo ao plano de ação e de resposta a incidentes no período, conforme procedimento interno da TI "TI-P032 - Procedimento para Reporte de Ocorrências de TI";
3. Relatório anual de atividades da TI referente aos testes realizados, incidentes, plano de ação e avaliação da estrutura;
4. Documentação sobre os procedimentos.

6.18 Violação da Política e Penalidades

No caso de não cumprimento das normas estabelecidas nesta política, o colaborador será comunicado que está infringindo as normas da Política de Segurança da Informação do Grupo GRECA e, poderá sofrer:

- Advertência verbal;
- Advertência escrita;
- Suspensão; ou
- Demissão por justa causa.

6.19 Trilhas de Auditorias

O processo de auditoria desempenha um papel fundamental na conformidade, integridade e segurança dos ativos, processos e dados do Grupo GRECA. Através dos procedimentos e trilhas de auditoria, aumentamos a auditabilidade dos ativos e demonstramos transparência nas atividades. Procedimentos devem ser disponibilizados para facilitar o processo de auditoria.

As trilhas de auditoria dos ativos podem ser encontradas nos Procedimentos TI-PXXX.

7. Considerações Finais

As dúvidas decorrentes de fatos não descritos nesta Política de Segurança da Informação deverão ser encaminhadas ao Comitê de Segurança da Informação para avaliação e decisão.

Esta PSI entra em vigor a partir da data de publicação e pode ser alterada a qualquer tempo, por decisão do comitê, mediante o surgimento de fatos relevantes que apareçam ou não tenham sido contemplados neste documento.

8. Histórico de aprovação e revisão do documento

Revisão	Data	Descrição da revisão
1.0	14/08/2020	Elaboração da política.
2.0	04/12/2020	Inclusão de um membro de Controles Internos para o Comitê de Segurança da Informação; Inclusão do compromisso da alta direção com melhoria contínua dos procedimentos relacionados à PSI no tópico 6.3; Liberação de uso de internet para uso recreativo durante horário de almoço conforme item 23 do tópico 6.5; Inclusão do tópico 6.16 que diz respeito a contratação de serviços em nuvem; Inclusão de demissão por justa causa como possível medida disciplinar no tópico 6.18.

3.0	26/11/2021	Atualização de resolução 4.658 para 4.893 do Banco Central do Brasil (BACEN), que dispõe sobre política de segurança cibernética e a contratação de serviços de processamento e armazenamento de dados em nuvem, nos tópicos 6.1, 6.16 e 6.17; Atualização do tópico 6.15, descrevendo o que configura situações de crise e o que fazer em caso de incidentes relevantes.
4.0	19/09/2023	Atribuição de responsabilidade de auditabilidade – tópico 3.4; Inclusão de acesso a rede visitante por voucher – tópico 6.5; Gestor poderá intermediar entrega da primeira senha de acesso, e abordado multifator de autenticação e aplicativo autenticador – tópico 6.6 e 6.7; Responsabilidade sobre danos em equipamentos pessoais e revogação de acesso à rede corporativa – tópico 6.9; Inclusão de considerações sobre procedimentos e trilhas de auditoria – tópico 6.19; Ajustes menores de termos e semântica.

9. Aprovação

Elaborado pelo Comitê de Segurança da Informação	
Departamento de TI Nome/Assinatura:	DocuSigned by: Fabio Boito 950D557EC0444C7... 11/24/2023
Departamento de Auditoria Interna Nome/Assinatura:	DocuSigned by: Rafael Santiago 3F24F107D8DB481... 11/24/2023
Departamento de RH Nome/Assinatura:	DocuSigned by: Janaina Assunção A456E72A3AF5460... 11/27/2023
Átria Financeira Nome/Assinatura:	DocuSigned by: 134037F32ADA47A... 11/24/2023
Aprovação da Diretoria Administrativa Nome/Assinatura:	DocuSigned by: Edenilson Dalbosco 6CDE16DF04D0436... 11/25/2023

ANEXO I
F004 – Termo de Ciência sobre a Política de Segurança da Informação

TERMO DE CIÊNCIA E RESPONSABILIDADE SOBRE A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NO GRUPO GRECA

Comprometo-me a:

1. Executar minhas tarefas de forma a cumprir com as orientações da Política de Segurança da Informação e com as Normas e Padrões vigentes;

2. Utilizar adequadamente os equipamentos do Grupo GRECA, evitando acessos indevidos aos ambientes computacionais aos quais estarei habilitado, de modo a não comprometer a segurança das informações;

3. Não revelar, fora do âmbito profissional, fatos ou informações de qualquer natureza que tenha conhecimento devido a minhas atribuições, salvo em decorrência de decisão competente do superior hierárquico;

4. Acessar as informações somente por necessidade de serviço e por determinação expressa do superior hierárquico;

5. Manter cautela quanto à exibição de informações sigilosas e confidenciais, em tela, impressoras ou outros meios eletrônicos;

6. Observar os procedimentos de segurança estabelecidos quanto à confidencialidade de minha senha;

7. Informar imediatamente o setor de TI ao ser observada qualquer não conformidade no uso de recursos de TI.

Informações detalhadas estão disponíveis no setor de TI do Grupo GRECA, ou na Intranet.

- PO001 - Política de Segurança da Informação
- TI-P001 - Governança de Tecnologia da Informação
- TI-P002 - Gestão de Serviços
- TI-P007 - Gestão de Acessos de TI
- TI-P009 - Gestão de Acessos à Internet
- TI-P010 - Procedimento para Disponibilização de Uso e Recursos de TI
- TI-P020 - Procedimento para Perda, Roubo ou Dano a Recursos de TI
- TI-P022 - Gestão de Segurança da Informação
- TI-P023 - Processo de Armazenamento e Manuseio Eletrônico de Arquivos
- TI-P024 - Plano de Contingência de TI
- TI-P025 - Procedimento de Acionamento de Disaster Recovery
- TI-P026 - Segurança Física do Data Center
- TI-P027 - Procedimento para Backup e Restore
- TI-P028 - Procedimento de Medidas Preventivas contra Vírus
- TI-P029 - Procedimento para Conexão de Equipamentos à Rede
- TI-P030 - Gestão de Riscos de TI
- TI-P032 - Procedimento para Reporte de Ocorrências de TI

Declaro estar ciente das determinações acima, compreendendo que quaisquer descumprimentos dessas regras podem implicar na aplicação de sanções disciplinares cabíveis.

Data: __/__/____ Nome: _____ Assinatura: _____