1 OBJETIVO

Apresentar uma visão abrangente de Segurança da Informação aplicada aos negócios, abordando conceitos e princípios essenciais que devem ser observados por todos, que de alguma maneira utilizem recursos tecnológicos, informações e/ou acessem fisicamente as dependências das empresas do Grupo Imagem, visando assegurar níveis elevados de proteções de seus ativos.

Esse documento complementa os manuais M-GQ-02 - Manual de Gestão - Vega, M-GQ-03 - Manual de Gestão – Geosistemas, M-GQ-04 - Manual de Gestão - Imagem Gestão e M-GQ-05 - Manual de Gestão - Codex Utilities.

2 ABRANGÊNCIA

Abrange os processos com seus colaboradores, diretores, executivos, acionistas, prestadores de serviços, fornecedores, parceiros diversos e demais contratados que estejam a serviço do Grupo Imagem.

3 DOCUMENTOS DE REFERÊNCIA

- M-GQ-02 - Manual de Gestão - Vega
- M-GQ-03 - Manual de Gestão - Geosistemas
- M-GQ-04 - Manual de Gestão - Imagem Gestão
- M-GQ-05 - Manual de Gestão - Codex Utilities
- P-PC-12 - Admissão
- PO-GOV-02 - Código de Conduta
- PR-GOV-04 - Due Diligence
- PO-GOV-06 - Política Sobre Conflito de Interesse
- PO-GOV-16 - Política de Privacidade
- PO-GOV-21 - Política de Segurança da Informação

- PR-GQ-08 - Ação Corretiva
- PR-GQ-13 - Gestão de Mudança
- PR-GQ-14 - Gestão de Riscos – Ferramenta AMMRisk
- PO-TI-03 - Política de Criptografia
- PO-TI-04 - Política de Backup e Disaster Recovery
- PO-TI-05 – Política de Gestão de acessos
- PR-TI-03 - Gestão de incidentes
- PR-TI-06 - Segurança física e do ambiente
- PR-TI-07 - Plano de Continuidade do Negócio - Geosistemas
- PR-TI-08 - Relacionamento com a cadeia de suprimentos
- PR-TI-09 - Dispositivos móveis e trabalho remoto
- PR-TI-10 - Gestão de Capacidade
- PR-TI-11 - Gestão de Vulnerabilidade Técnica
- PR-TI-14 - Plano de Continuidade do Negócio – Vega Monitoramento
- PR-TI-15 – Orientação para troca de senhas
- PR-TI-16 - Orientação para criação de usuários
- P-TI-02 - Contratação de Colaboradores e Entrega de Ativos
- P-TI-06 – Desligamento de Colaboradores e Devolução de Ativos
- PR-PS-03 - Processo de Desenvolvimento Seguro
- PO-OPE-01 - Política de Desenvolvimento Seguro
- P-OPE-01 - Desenvolvimento Seguro
- F-TI-04 - Validação de Permissão
- NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação – Requisitos;
- NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação.

4 DEFINIÇÕES

- **Segurança da Informação:** é a disciplina que envolve um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware, para garantir que a confidencialidade, integridade e disponibilidade das informações sejam preservadas;
- **Confidencialidade:** propriedade que a informação tem de que não será divulgada às entidades e/ou pessoas não autorizadas;
- **Integridade:** um princípio que garante que a informação e/ou itens de configuração somente sejam modificados por pessoas autorizadas;
- **Disponibilidade:** propriedade que a informação tem de que estará disponível para às entidades e/ou pessoas autorizadas, no momento requerido;
- **Ativo:** é algo que tem valor para a organização e que, portanto, requer proteção, compreende mais do que hardware e software.
- **Informação**: é um ativo que, como outros, consequentemente, precisa ser adequadamente protegido;
- **Ameaças**: causa potencial (agente) de um incidente indesejado que pode resultar em dano para um sistema ou organização. Podem colocar em risco a confidencialidade, integridade e disponibilidade das informações. São classificadas em naturais, intencionais e involuntárias;
- **Vulnerabilidades**: fragilidades de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;
- **Riscos**: é a probabilidade de ameaças explorarem vulnerabilidades, causando perdas ou danos aos ativos e, consequentemente, impactos aos negócios;
- **Incidente de Segurança da Informação**: Evento não planejado que pode acarretar prejuízos à empresa ou mesmo violar as regras de segurança;
- **Comitê de Segurança da Informação**: Grupo que contribui nas decisões e ações relacionadas com a segurança da informação;

5 RESPONSABILIDADES

O Grupo Imagem, por intermédio do Conselho Consultivo (Órgão Diretivo), Diretoria Executiva (Alta Direção) afirma seu compromisso para com a segurança da informação, leis e regulamentações aplicáveis ao negócio, para tanto, desenvolveu Políticas de Gestão, Política de Governança, Política de Privacidade de Dados e Política de Segurança da Informação.

Estabeleceu objetivos e metas, disponibiliza os recursos necessários para o atendimento aos requisitos, promove a abordagem de processo e mentalidade de riscos.

O Código de Conduta do Grupo Imagem estabelece as regras e orientações para interação dos colaboradores no ambiente interno e externo, expressa a Missão, Visão e Valores do grupo, está aderente as normas de responsabilidade social, proteção de dados e segurança da informação e processos da empresa.

A liderança assegura a gestão dos recursos necessários para garantir a manutenção e a melhoria contínua do Sistema de Gestão, conduz as análises críticas gerenciais e se responsabiliza por prestar contas pela sua eficácia.

A área de Pessoas & Cultura mantém as descrições dos cargos, onde se detalham os papéis e responsabilidades dos colaboradores e os termos de concordância com as políticas e diretrizes internas.

Foram estabelecidos controles para evitar situações conflitantes e garantir a segregações de funções detalhadas PR-GOV-04-Due Diligence, PO-GOV-06 - Política Sobre Conflito de Interesse.

O Gestor da TI é responsável pelo sistema de segurança da informação e reporta resultados na análise crítica anual do sistema.

Para garantir um nível de proteção adequado aos sistemas e informações, foi definido que todos os acessos dos usuários (comuns e privilegiados) devem ser devidamente registrados, aprovados pelos responsáveis e revisados periodicamente conforme estabelecido no procedimento PO-TI-05 – Política de Gestão de Acessos.

5.1 RESPONSABILIDADES DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO

O Comitê Segurança da Informação é formado por uma equipe multidisciplinar e tem como responsabilidades:

- Contribuir com as decisões e ações relacionadas com a segurança da informação;
- Apoiar na revisão da Política de Segurança da Informação;
- Interagir com grupos, associações profissionais ou outros fóruns especializados em segurança da informação;
- Assessorar na disseminação das práticas de Segurança da Informação;
- Propor soluções, processos, controles e indicadores específicos sobre segurança da informação;
- Apoiar na análise e controle dos riscos, no gerenciamento de Incidentes e na efetividade do Plano de Continuidade do Negócio;

As demais responsabilidades relacionadas para com o SGSI estão descritas nos procedimentos documentados que tem uma seção específica para esta finalidade.

5.2 RESPONSABILIDADES DE COLABORADORES E PRESTADORES DE SERVIÇOS

- Proteger os ativos de informação e relatar qualquer situação que represente desvio ou violação de segurança deles, bem como atender às recomendações pertinentes constantes na Política de Segurança da Informação.
- Responsabilizar pelo equipamento que utiliza e solicitar chamados junto ao TI em caso de defeito utilizando para isso o Sistema TopDesk.

6 PRINCÍPIOS

A fim de alcançar seu objetivo em relação ao sistema de Gestão da Segurança da Informação, o Grupo Imagem estabelece os seguintes princípios fundamentais:

- A responsabilidade pela segurança da informação é de todos os colaboradores;
- Os ativos de informação devem-se ser utilizados de maneira ética e profissional por todos;
- Acesso aos ativos de informação somente por pessoas autorizadas, respeitando a sua confidencialidade;
- Deve-se manter a Integridade das informações durante todo o seu ciclo de vida, ou seja, desde sua criação até seu descarte;
- Estar em conformidade com regulamentações, legislações, políticas e normas organizacionais.

7 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação (PO-GOV-21 - Política de Segurança da Informação) define os compromissos do grupo Imagem e suas principais diretrizes.
Foi estabelecida visando o atendimento a um sistema de gestão de segurança da informação que contemple todo o controle e operação dentro do grupo Imagem e foi aprovado pelo Conselho consultivo.

8 PREMISSAS

A concepção do sistema de gestão de segurança da informação, conforme requisitos estabelecidos pela norma NBR ISO IEC 27001:2013 se baseia num processo de gestão de riscos (avaliação, controle e tratamento de incidentes/emergências) relacionados com os ativos de informações e na gestão do capital humano. Os detalhes da aplicação de cada processo e/ou atividade de controle estão elencados abaixo.

8.1 AVALIAÇÃO DE RISCOS

A avaliação dos riscos relacionadas à segurança da informação é conduzida conforme diretrizes estabelecidas no procedimento PR-GQ-14 – Gestão de Riscos – Ferramenta AMMrisk. Os riscos são controlados e registrados no Sistema AMMrisk.

8.2 TRATAMENTO DOS RISCOS – MATRIZ DE APLICABILIDADE

O tratamento dos riscos leva em conta os controles sugeridos no Anexo A da ISO 270001.

A Declaração de Aplicabilidade fica registrada no documento F-TI-19 - Declaração de Aplicabilidade do SGSI – Vega Monitoramento. Os detalhes do tratamento dos riscos estão descritos no procedimento PR-GQ-14 – Gestão de Riscos – Ferramenta AMMrisk.

8.3 SEGURANÇA EM RECURSOS HUMANOS

Está estruturado um processo para contratação de colaboradores, conforme diretrizes definidas no documento P-PC-12 Admissão.

Profissionais designados (exemplos: representantes da qualidade, TI e comitê de segurança da informação) recebem capacitação em Sistema de Gestão da Segurança da Informação (norma ISO 27001) e atualização regular nas políticas de segurança da informação.

O programa de conscientização em segurança da informação e proteção de dados é realizado através de workshops, publicações internas e de forma sistemática através dos Onboarding de novos colaboradores e reciclagens realizadas no mínimo a cada 2 anos.

Casos de violações de segurança da informação por parte dos colaboradores serão investigados e estarão sujeitos à processos disciplinares, conforme diretrizes estabelecidas no PO-GOV-02 - Código de Conduta.

8.4 DISPOSITIVOS MÓVEIS E TRABALHO REMOTO

O documento PR-TI-09 – Dispositivos Móveis e Trabalho Remoto, foi estabelecido para garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis.

As mudanças no ambiente computacional (que envolvem hardware, sistema operacional, substituição ou atualização de aplicativos) são executadas e controladas conforme os documentos PR-GQ-13 - Gestão de Mudança e o respectivo formulário de gestão de mudança da empresa associada.

A capacidade de processamento dos equipamentos e sistemas são realizadas através do levantamento da capacidade fluxo de dados, processamento, armazenamento e dos alertas emitidos por cada sistema.

A separação de ambientes para desenvolvimento e testes segue a sistemática descrita nos documentos fluxos de processos do departamento de Soluções (Imagem Geosistemas) e departamento de Operações (Vega Monitoramento).

8.5 GESTÃO DE ATIVOS

Os ativos são mapeados e controlados através da ferramenta AMMRisk e no Software Sistema de Inventário.

Eles são divididos por tipos e rotulados como públicos, restritos ou confidenciais.

Todos os ativos possuem um responsável, que deve seguir as diretrizes estabelecidas nos processos e controles implementados (PO-GOV-02 - Código de Conduta, F-TI-02 – Termo de entrega de Equipamento, F-PC-17 - Aditivo ao Contrato De Trabalho - da Proteção de Dados Pessoais e Segurança da Informação e PO-GOV-21 - Política de Segurança da Informação), os quais provem as proteções requeridas, incumbindo-os do uso aceitável dos ativos sob sua responsabilidade e das ações necessárias para a mitigação dos riscos associados.

Além disso, periodicamente, são realizados workshops abordando o tema de segurança da informação, no qual são reforçadas tais diretrizes estabelecidas.

Cada ativo listado na ferramenta AMMRisk, tem seus detalhes e informações descritos para facilitar o processo de avaliação de riscos, conforme PR-GQ-14 - Gestão de Riscos – Ferramenta AMMrisk.

No encerramento de contratos de trabalhos, é utilizado o fluxo descrito em P-TI-06 – Desligamento de Colaboradores e Devolução de Ativos, para garantir que todos os ativos que estavam em posse dos colaboradores sejam devolvidos para a organização.

O inventário dos ativos é analisado criticamente na frequência anual para verificar a sua adequação e pertinência.

8.6 CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

O proprietário da informação é responsável por classificá-la adequadamente aplicando o nível de proteção proporcional a sua importância e por rotulá-la com o nível de segurança adequado, conforme tabela abaixo.

As informações só podem ser divulgadas externamente quando autorizadas pelo proprietário, salvo quando envolver ordens judiciais.

As informações, em especial dados pessoais (incluindo as sensíveis), devem ser utilizadas unicamente para a finalidade para a qual foram coletadas, conforme diretrizes da LGPD.

As informações do Grupo Imagem, ou de sua responsabilidade, devem ser classificadas de acordo com seu valor para o negócio e sensibilidade utilizando os níveis de segurança apresentados abaixo:

Nível de Segurança	Rótulo	Critérios de Classificação	Quem pode acessar
Público	Não se aplica	Tornar a informação pública não prejudica o Grupo Imagem. O documento NÃO contém dados pessoais ou dados pessoais sensíveis	Qualquer pessoa
Restrito	Informação interna	O acesso não autorizado às informações pode causar pequenos danos e/ou inconvenientes para o Grupo Imagem. Alguns documentos podem conter dados pessoais.	Apenas colaboradores e prestadores de serviços autorizados
Confidencial	Informação confidencial	O acesso não autorizado às informações pode causar danos consideráveis aos negócios e/ou à reputação do Grupo Imagem. Os documentos podem contém dados pessoais sensíveis.	Apenas o dono do documento e demais pessoas por ela autorizadas

O proprietário da informação é responsável por assegurar que as informações estejam controladas de forma a garantir que apenas as pessoas autorizadas possam acessá-las.

Os dados lógicos confidenciais têm restrições que só permitem o acesso por pessoas autorizadas.

As informações analógicas confidenciais têm controle de acesso para as salas e foram colocados rótulos de confidencial nos armários. Quando armazenados externamente, são selecionadas empresas que garantam a segurança da informação.

Os procedimentos, fluxos e manuais, são restritos as empresas de grupo e partes interessadas. No sistema de armazenamento dos documentos, são identificados os rótulos de classificação da informação.

Todas as categorias de informações têm processos para proteção da integridade e disponibilidade.

8.7 GESTÃO DE ACESSOS

A gestão dos direitos, alteração e revogação de acessos aos ativos é cadastrada e controlada. As regras estão documentadas no PO-TI-05 – Política de Gestão de Acessos.

8.8 CRIPTOGRAFIA

Os equipamentos portáteis estão cobertos pelas rotinas de criptografia, conforme diretrizes do PO-TI-03 – Política de Criptografia.

8.9 SEGURANÇA FÍSICA E DO AMBIENTE

Foram definidos os controles para prevenir o acesso físico nas dependências da empresa e no datacenter, de forma a manter os recursos essenciais para a operação segura dos ativos e evitar danos e interferências nos recursos de processamento das informações.

A infraestrutura necessária para operação segura dos ativos é gerenciada e os recursos críticos são controlados e submetidos a manutenções regulares para assegurar o seu pleno funcionamento, conforme diretrizes estabelecidas pelo PR-TI-06 - Segurança Física e do Ambiente.

8.10 SEGURANÇA NAS OPERAÇÕES

Os colaboradores são orientados quanto à importância dos cuidados com as informações em elevadores, restaurantes, aeroportos, aviões ou em outros lugares públicos.

Para que seja permitido a troca de informações entre o Grupo Imagem e partes externas, são estabelecidos acordos de confidencialidades.

O uso de sistemas de comunicações eletrônicas, e todas as mensagens geradas ou transmitidas através do mencionado sistema, são considerados propriedade do Grupo Imagem. O acesso à caixa de Correio Eletrônico se dará através de software específico, cuja configuração será feita pelo Departamento de Tecnologia da Informação.

A TI valida com presidente do conselho do Grupo Imagem as regras de bloqueio dos sites.

Se houve necessidade de desbloqueio de site, o gestor deve abrir chamado, justificando o motivo. A TI vai analisar o risco e informar a liberação ou não no chamado.

O conteúdo e o uso de sistemas de comunicações eletrônicas são monitorados para apoiar as atividades de manutenção, segurança, auditoria e outras investigações. Os usuários devem utilizar as comunicações eletrônicas tendo em mente o fato de que o Grupo Imagem se reserva o direito de examinar o conteúdo delas.

É responsabilidade do usuário, ao receber mensagens de origem desconhecida ou que contenham arquivos anexos duvidosos, não abrir ou executar tais anexos e encaminhar tal mensagem imediatamente para o Departamento de Tecnologia da Informação.

8.10.1 PROTEÇÕES CONTRA MALWARES

As estações de trabalho do grupo Imagem possuem solução de antivírus instalada e gerenciada através de uma plataforma que integra todos os logs de atividades suspeitas e de ameaças de softwares maliciosos, impedindo a ação de malwares e fazendo as verificações em arquivos e/ou dispositivos de mídia.

A plataforma de gerenciamento distribui atualizações sempre que necessário. A partir dessa plataforma é possível visualizar todas as máquinas e qualquer ação suspeita.

Todos os novos colaboradores recebem no Onboarding a orientação sobre os riscos referentes a vírus e as melhores práticas de comportamento seguro na rede, devendo tomar precauções para evitar a contaminação dos computadores.

8.10.2 CÓPIAS DE SEGURANÇA

O Grupo Imagem conta com um sistema de backup totalmente automatizado, realizando backups da Infraestrutura de máquinas e arquivos, da informação relevante para operação dos negócios do Grupo Imagem conforme descrito no documento PO-TI-04 – Política de Backup e Disaster Recovery.

8.10.3 REGISTROS E MONITORAMENTOS DE EVENTOS

O registro e a proteção dos eventos de logs de todos os usuários são realizados para os principais sistemas do Grupo Imagem (AD, Sharepoint, Firewall, Fileserver) através do software SIEM (Security Information and Event Management).

Quando o login é efetuado no servidor é gerado um log (registro de entrada e saída). A análise é realizada através da visualização dos dashboards de cada aplicação e quando necessário, sob demanda.

Os usuários com acessos privilegiados não conseguem excluir as evidências do seu próprio log (sistemas AD e Fileserver) do registro no software SIEM (Security Information and Event Management).

O software do SIEM mantém esse registro de logs por um período de 6 meses, o que permite a rastreabilidade de qualquer log de usuário privilegiado.

Os serviços e atividades são monitorados em regime 24 horas x 7 dias, assegurando a gestão sobre vulnerabilidades técnicas.

A TI implementou processo interno com um conjunto de atividades coordenadas de análise e correção para reduzir a níveis aceitáveis, as vulnerabilidades de segurança encontradas no ativo, conjunto de ativos ou ambiente. Detalhes estão no processo PR-TI-11 - Gestão de Vulnerabilidades Técnicas.

8.10.4 SINCRONIZAÇÃO DE RELÓGIO

O relógio do Active Directory (AD) é sincronizado com o servidor de horas do Brasil (NTP.br) que sincroniza com o relógio de todas as máquinas do Grupo Imagem.

8.10.5 INSTALAÇÃO PADRÃO

A instalação inicial dos sistemas é orientada através do uso do F-TI-16 - Check List de Preparação de Equipamento.

Um conjunto padrão de instalação de software é preparado e mantido em local seguro. Estas cópias padrão são usadas para a recuperação de infecções de vírus, falhas do disco rígido e outros problemas do equipamento.

O F-TI-16 - Checklist de Preparação de Equipamento também contempla a configuração (formatação de máquina ou disponibilização de nova máquina) no perfil do usuário (configuração do Outlook e Onedrive).

O uso ou instalação de software ou hardware só é permitido quando devidamente homologado e licenciado.

A instalação de softwares é permitida somente para os seguintes setores, os quais possuem perfil de administrador local:

- Imagem Geosistemas: Professional Services, Suporte e Marketing de Produtos;
- Vega Monitoramentos: Operações.

Os demais setores terão perfil ajustado de forma que não consigam instalar nenhum software, de modo que terão de abrir chamado pata TI no Topdesk para instalação. Todos os colaboradores são monitorados e em caso de identificação de software não licenciado, a equipe da TI notifica o usuário e depois verifica se foi desinstalado, ou se foi adquirido.

Softwares são utilizados para a realização de inventário de instalações e uso de softwares, com o intuito de verificar e identificar possíveis instalações não permitidas.

8.10.6 AUDITORIAS DE SISTEMA DA INFORMAÇÃO

As auditorias de sistema são realizadas anualmente e o registro é armazenado no repositório da TI.

Eventuais não conformidades identificadas serão registradas e tratadas conforme as diretrizes do documento PR-GQ-08 - Ação Corretiva.

Além das auditorias é realizada a verificação e registrado o monitoramento de forma constante através dos alertas de segurança sistêmicos.

Os resultados das auditorias são submetidos ao Gestor de TI, que avalia e informa ao Diretor Executivo.

8.11 SEGURANÇA NAS COMUNICAÇÕES

A rede corporativa do Grupo Imagem possui implementações de segurança que impedem que pessoas externas à organização acessem seus recursos.

Para acessar a rede é necessário autenticação através de login e senha.

A rede é monitorada por Sistemas que verificam os principais serviços e servidores, emitindo alertas caso identifique alguns problemas de performance e/ou inatividade.

Os recursos listados no inventário de ativos tecnológicos devem ser mantidos em condições adequadas de funcionamento no Sistema AMMrisk.

Os ativos tecnológicos externos são controlados conforme diretrizes estabelecidas em contratos com os fornecedores destes dos ativos e/ou serviços.

8.11.1 ACESSO REMOTO

Todo o acesso remoto aos sistemas do Grupo Imagem é feito, obrigatoriamente, através de VPN (Virtual Private Network).

Todo equipamento que necessite acessar a rede do Grupo Imagem remotamente deve possuir software cliente de VPN homologado e será autorizado e monitorado pelo Departamento de Tecnologia da Informação.

8.11.2 SEGREGAÇÃO DE REDES

O endereçamento dos equipamentos conectados à rede é dinâmico e os IPs são atribuídos automaticamente. A utilização de endereços fixos somente ocorre quando autorizados pelo Gestor de TI.

8.11.3 SERVIÇOS DE REDE TERCEIRIZADOS

Os serviços de rede de terceiros são documentados e a segurança é verificada previamente. Os novos sistemas ou redes de acesso com acesso às redes externas ao Grupo Imagem devem ser solicitadas pelo Responsável pelo Contrato e através do Sistema Topdesk.

8.11.4 ACORDOS DE CONFIDENCIALIDADE

Acordos de confidencialidade deverão ser firmados com os colaboradores e prestadores de serviços ligados aos ativos relevantes para a segurança da informação.

8.12 DESENVOLVIMENTO SEGURO

Princípios de desenvolvimento seguro foram validados para reforçar a importância do tema segurança aplicado ao ciclo de vida dos projetos de desenvolvimento de software.

Foram definidos os padrões mínimos de requisitos de segurança para prevenção a ataques a sistemas.

Os requisitos são verificados antes da entrega para o cliente e eles são repassados quando o desenvolvimento é terceirizado.

As diretrizes para a **Imagem Geosistemas** estão documentadas no PR-PS-03 Processo de Desenvolvimento Seguro e para **Vega Monitoramento** no PO-OPE-01– Política de Desenvolvimento Seguro.

8.13 RELACIONAMENTO DA CADEIA DE FORNECIMENTO

Foram definidos processos para orientar os fornecedores do grupo Imagem que possuem relação com os ativos de informação sobre as diretrizes de segurança da informação, bem como conscientizá-los sobre o correto uso dos recursos da organização.

As instruções e regras protegem os ativos de informações disponibilizadas pelo grupo Imagem, assim como a segurança dos recursos tecnológicos, ambientes e dependências acessados pelos fornecedores, garantindo a correta custódia e prevenindo ameaças deliberadas ou acidentais.

As diretrizes estão descritas no PR-TI-08 Relacionamento na Cadeia de Fornecimento.

8.14 GESTÃO DE INCIDENTES

Promover um ambiente onde todos se comprometem com segurança da informação é extremamente importante e exige um processo contínuo de conscientização.

É responsabilidade de todos informarem possíveis violações das Diretrizes de Segurança da Informação.

O documento PR-TI-03 Gestão de Incidentes estabelece as diretrizes para investigação e tratamento de incidentes.

8.15 GESTÃO DA CONTINUIDADE DO NEGÓCIO

Foram definidas as diretrizes para prevenir a interrupção das atividades do negócio e proteger os processos críticos contra defeitos, falhas ou desastres significativos, assegurando a retomada dos serviços e sistemas.

O Plano de Continuidade do Negócio estabelece as regras para administração de crises, contingências e recuperação de desastres. Os detalhes estão descritos no procedimento PR-TI-07 Plano de Continuidade do Negócio - Geosistemas e PR-TI-14 Plano de Continuidade do Negócio - Vega Monitoramento.

8.16 CONFORMIDADE

Os requisitos legais, regulamentares e contratuais pertinentes são identificados e mantidos devidamente atualizados, conforme descrito nos Manuais de Gestão.

Os registros são controlados conforme sistemática definida no procedimento de controle de informação documentada PR-GQ-01 - Controle de Informação Documentada.

Uma política de privacidade foi estabelecida e controles foram implementados para proteger adequadamente os dados pessoais, conforme requerido pela Lei Federal 12.379/2018.

Para a análise da conformidade técnica é realizado teste nos sistemas, como:

- Pentest: contratada uma empresa especializada, que realiza a atividade utilizando ferramenta automática e gera relatório, que subsidiam os planos de ajustes, correção dos processos, controles da TI e análise crítica.

- Teste de Vulnerabilidade: realizado internamente, utilizando uma ferramenta automática que gera relatório, que subsidiam os planos de ajustes, correção dos processos, controles da TI e análise crítica.

As análises críticas de segurança da informação são realizadas conforme critérios definidos nos Manuais de Gestão.