VISÃO GERAL DOS PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

Informar a clientes e parceiros a visão geral dos processos de segurança.

2. RESPONSÁVEL

A área de Segurança da Informação é responsável pela atualização desse documento.

3. NORMATIZAÇÕES

3.1. Gestão de Mudanças

As mudanças a serem realizadas no ambiente da AGE são planejadas, acompanhadas e revisadas, a fim de minimizarmos o impacto das alterações na disponibilidade e qualidade do serviço.

A mudança a ser executada é relacionada aos ativos, riscos e impactos envolvidos, tempo de execução das tarefas, responsáveis pelas tarefas e planejamento de rollback. Após avaliação e aprovação dos gestores ou alta direção, será executada a mudança.

Todo o processo de gestão de mudança (GMUD) é registrado, evidenciando o cumprimento de todas as etapas.

3.2. Gestão de Incidentes

Reportar incidentes de segurança da informação e privacidade, a fim de garantir que cada incidente seja gerenciado de forma consistente em toda a empresa, utilizando procedimentos e critérios de elegibilidade, comunicação eficaz, transparência, com intuito de conter os impactos na organização e nos serviços prestados.

O incidente pode ser formalizado através de e-mail, telefone ou processo, evidenciando assim todo andamento de análise e resolução.

Na etapa de gerenciamento de incidentes temos a identificação, registro, classificação de severidade, priorização de acordo com urgência e/ou impacto. Em seguida inicia-se investigação e diagnósticos, resolução imediata ou de contorno e plano de ação resolução e recuperação e encerramento.

A equipe de segurança da informação e Monitoramento emprega diagnostico padrão do ambiente para resolução de eventos que afetem o serviço. Os colaboradores fornecem apoio e suporte para detectar incidentes e gerenciar o impacto e a resolução.

3.3. Análise, Avaliação e Tratamento de Risco de Segurança da Informação

Foi integrado um programa de risco e conformidade em toda organização, visando gerenciar o risco em todos os processos, melhorar e reavaliar continuamente as atividades relacionadas aos serviços entregues e aplicação.

Avaliações e monitoramento de riscos são executados rotineiramente. Identificado algum risco, será analisado e mitigado.

A implementação de uma ampla gama de controles de segurança e ferramentas automatizadas, monitoramento e avaliação contínua dos controles de segurança ajudam a garantir a eficácia operacional.

Auditorias de conformidades, interna e externas, são realizadas por terceiros para avaliação do sistema de gestão de segurança da informação e privacidade, assim como testes de penetração – EHT.

3.4. Controle de Acesso

Regulamenta a gestão de usuários, sua identificação e acessos a sistemas da AGE.

A rede de produção da AGE é separada da rede corporativa. Foram estabelecidas procedimentos e políticas formais para delinear as normas mínimas de acesso lógico aos hosts da plataforma e da infraestrutura.

As políticas também identificam as responsabilidades funcionais pela administração do acesso lógico e de segurança.

Foi estabelecida política de credenciais com os intervalos de expiração as configurações necessárias. Além de complexas, as senhas são alteradas periodicamente.

3.5. Gestão de Ativos

Normatiza a gestão e monitoramento dos ativos da AGE, incluindo informação, computadores e demais recursos, com base na legislação vigente e nas medidas de blindagem contra riscos e práticas abusivas de terceiros.

Os ativos de informação são inventariados, classificados e protegidos de acordo com seu valor, requisitos legais, sensibilidade e criticidade para a organização. Todo ativo tecnológico tem as atualizações e correções de segurança do sistema operacional ou aplicativos devidamente validados. Os sistemas e computadores possuem versões instaladas, ativadas e atualizadas permanentemente pelo software de antivírus.

O monitoramento de equipamentos eletrônicos para detecção de atividades não autorizadas e vulnerabilidades são devidamente registrados. Sistemas de monitoramento são implantados no parque tecnológico de acordo com as necessidades de monitoramento especificas. Temos instalados sistemas

de proteção e detecção de invasão para garantir a segurança das informações e dos perímetros de acesso.

Os resultados das atividades de monitoramento são analisados criticamente e de forma regular. Os registros de logs são armazenados, a fim de auxiliar em futuras investigações e monitoramento.

As mídias removíveis da AGE são controladas. O descarte de mídias é realizado de forma segura (triturado, incinerado etc.) de modo que não possam ser recuperados.

3.6. Tecnologia da Informação e uso aceitável de ativos

Visa regulamentar as responsabilidades de tecnologia da Informação e o uso aceitável de ativos da AGE.

A AGE possuí um departamento responsável por toda gestão (aquisição, configuração e homologação de equipamentos relacionados ao uso de tecnologias necessárias à comunicação, manuseio e armazenamento de informações); pela guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação; pelas cópias de segurança dos programas e dados e pela proteção contínua dos ativos de informação da empresa contra códigos maliciosos.

O Plano de recuperação de desastres de TI (DR), é testado e atualizado anualmente. Mantendo-se alinhado com a realidade e objetivos de negócio da AGE, garantindo a continuidade dos serviços críticos de tecnologia da informação, independentemente das situações e adversidades enfrentadas.

Para mitigar possíveis problemas a AGE utiliza controles de segurança adequados em sua administração, tais como, mas não se limitando a: segregação de responsabilidades operacionais; uso de criptografia e protocolos de segurança; sistemas de detecção de invasão e/ou sistemas de prevenção; aprova e testa as conexões de rede, serviços, protocolos e portas de comunicação permitidas e alterações às configurações do firewall e do roteador; analisa os conjuntos de regras do firewall e de roteadores anualmente; mantém um diagrama da rede atualizado com todas as conexões e monitora os equipamentos e/ou softwares com capacidade para analisar tráfego de rede.

Dentro do ambiente da AGE algumas restrições foram implementadas para manter a segurança dos ativos de informações.

O acesso remoto à rede e às informações é feito por meio de ferramentas homologadas e implementadas pela área de Tecnologia da Informação.

3.7. Cópias de Segurança

A extração de cópias de segurança, utiliza de meios (físicos ou eletrônicos) que asseguram a integridade de informações consideradas vitais para o sistema e para a retomada das atividades da área em caso de contingência.

Existem dois tipos de backup:

Backup Interno são as cópias de segurança dos dados do escritório sede e demais unidades de negócio da AGE necessárias ao retorno das atividades dos colaboradores e parceiros. As cópias de segurança são protegidas através de criptografia.

Backup Externo são as cópias de segurança dos dados dos servidores de produção necessários para o funcionamento do Sistema SOC. As cópias são feitas em meios eletrônicos, ocorrendo um rodízio, para que possa ser respeitado o período de retenção definido para os conjuntos de cópias de segurança. As cópias de segurança são protegidas através de criptografia.

Os conjuntos de cópias de segurança são testados regularmente. Os testes geram evidências do sucesso da restauração da amostra selecionada, como logs ou comprovação de integridade dos dados. Os testes são realizados em ambiente dedicado para evitar sobrescrever os dados originais e, em caso de falha no processo de restauração, causar danos irreparáveis ou perda de dados.

3.8. Mesa limpa e tela protegida

Regulamenta a limpeza nas mesas e a proteção das telas, visando a integridade de informações.

Diretrizes são aplicadas em toda empresa, de modo que papéis/documentos não fiquem expostos a acessos não autorizados. Papéis e mídias de computador são guardados, quando não estiverem sendo utilizados.

Os terminais de computador e impressoras são desligados quando desassistidos, os equipamentos são protegidos por mecanismo de travamento de tela por senhas, chaves ou outros mecanismos de autenticação quando não estão em uso.

3.9. Segurança física e ambiente

Tem como premissa garantir que o acesso físico as instalações onde os ativos de TI e informações críticas a continuidade do negócio estejam armazenados sejam controlados de forma a garantir a sua proteção, disponibilidade, integridade e confidencialidade. Alguns locais dependendo da sua maior criticidade em relação ao impacto na continuidade do negócio da AGE poderão necessitar de um nível adicional de proteção ou tratamento especial.

Para evitar acesso não autorizado, dano ou interferência aos sistemas de informação um perímetro de segurança foi definido. Barreiras físicas e sistemas de controle de acesso foram implementados para garantir o acesso apenas por usuários autorizados. O acesso ao ambiente interno só é permitido quando devidamente autorizado, por biometria e identificação.

Todo perímetro de segurança possuí detecção de fumaça, alarme de incêndio, climatização, nobreak, cabeamento protegido e monitoramento.

3.10. Classificação e manuseio de informações

Os ativos de informação da AGE estão protegidos de acordo com as seguintes classificações e rotulagens determinadas: Pública, Sensível, Privada e Confidencial.

Informações Privadas e Confidenciais são acessadas somente pessoas autorizadas e que realmente necessitam da informação, que tenham o Acordo de Não Divulgação de Informações (Termo de Confidencialidade) firmado com a organização. As informações Privadas ou Confidenciais são transmitidas criptografadas.

Informações Públicas são Informações que não necessitam de uma proteção especial. Informação que pode ser divulgada a qualquer pessoa, sem violar o direito à privacidade.

Informação Sensível são informações que devido à sensibilidade técnica ou de negócio exigem cuidados especiais para garantir a integridade dos dados, protegendo-a de modificação ou destruição não autorizada. Essas informações destinam-se ao uso interno da organização, e seu acesso deve ser limitado a clientes, fornecedores e parceiros críticos.

Para classificação das informações, as responsabilidades foram implementadas em quatro níveis: Proprietário, Custodiante, Usuário e Equipe de Segurança. As informações privadas ou confidenciais são destruídas de tal forma que se torne ininteligível e inutilizável.

De acordo com a classificação da informação existe um tipo de acesso, copia, rotulagem, armazenamento, guarda, destruição e descarte. Possuindo assim um ciclo de vida da informação.

3.11. Desenvolvimento e projetos de sistemas seguros

Norteia as ações e responsabilidades antes, durante e depois o processo de desenvolvimento seguro por parte da AGE e/ou terceiros, e/ou aquisição de softwares.

Os responsáveis técnicos participam em fases-chave do Ciclo de Vida do Desenvolvimento do Software para garantir os requisitos e medidas de segurança apropriadas.

Os ativos de informação em desenvolvimento ou em fase de mudanças passam por uma avaliação de riscos de segurança da informação, durante a sua fase de planejamento do projeto, para identificar os requisitos de segurança apropriados. Tais requisitos são definidos com base nos riscos identificados; nos requisitos legais e regulamentares para a proteção de dados.

Controles de segurança da informação são estabelecidos para proteger os ativos de informação, durante o desenvolvimento e a manutenção do software.

Testes de segurança são realizados considerando a confidencialidade, integridade e disponibilidade das informações do software. Os testes de segurança são realizados antes dos softwares serem colocados no ambiente de produção.

Os testes são realizados em um ambiente de homologação seguro e apartado. São realizados testes a nível de código, para todos os softwares novos ou significativamente modificados, em especial para aqueles que afetam a coleta, uso e/ou a exposição de dados confidenciais.

3.12. Correio eletrônico

Regulamenta o uso do correio eletrônico (e-mail) dos colaboradores. O uso do Correio Eletrônico (e-mail) e o comunicador instantâneo é destinado a fins corporativos. Toda entrada de e-mail na rede da empresa passa por software antivírus para resguardar a segurança. O envio de arquivos com dados confidenciais e sensíveis, são realizados utilizando arquivos criptografados. A área de Tecnologia da Informação efetua o monitoramento de comunicações eletrônicas, que é realizado exclusivamente com a finalidade de proteger ativos de informação de propriedade da AGE, bem como validar o respeito às regras expostas nesta norma e na legislação em vigor.

4. OUTRAS NORMAS

Possuímos também, outras normas que nos auxiliam a manter a segurança de nossos ativos de informação. As normas são baseadas nas melhores práticas de segurança e atende a ISO 27.001:2013:

- **Norma de Fornecedores;**
- **Norma de Conformidades;**
- **Norma de Conduta Ética de Colaboradores;**
- **Norma de Indicadores de SGSIP.**