

Política de Segurança da Informação



	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	2 / 35

Conteúdo	Pag.
1- Introdução.....	04
2- Responsabilidade.....	05
3- Compromissos de Gestão.....	06
4- Políticas de segurança informática.....	06
5- Políticas de segurança para comunicações.....	08
6- Políticas de segurança de rede.....	08
7- Gestão de Segurança da Informação.....	11
8- Política de Segurança Específica.....	12
8.1 Segregação de funções.....	12
8.2 Contato com as autoridades.....	12
8.3 Segurança da informação na gestão de projetos.	12
8.4 Política de controle de acesso.....	13
8.5 controle de acesso a redes e serviços associados.....	13
8.6 Solicitação de Acesso.	13
8.7 Identificação de Perfis.	14
8.8 Novos Acessos.	14
8.9 Revisão de Atividades (log).	15
9- Procedimentos e políticas específicas.....	15
9.1 Política de Dispositivos Móveis.....	15
9.2 Política de Uso Aceitável.....	15
9.3 Política de Classificação de Informações.....	16
9.4 Política de Transferência de Informações.....	16
9.5 Procedimento para Trabalho em Área Segura.....	16
10- Criptografia.....	17
10.1 Controles criptográficos.	17
10.2 Política sobre uso de controles criptográficos.....	17
10.3 Gerenciamento de chaves.....	17
10.4 Formato Chave.....	17
10.5 Criptografia de Chave.....	17
11- Segurança Vinculada aos Recursos Humanos.....	18
11.1 Antes da contratação.....	18
11.2 Investigação de antecedentes.....	18
11.3 Termos e condições do contrato.....	18
11.4 Durante o contrato.....	18
11.5 Conscientização, educação e treinamento em segurança da informação.....	18
11.6 Processo disciplinar.....	18
11.7 Rescisão ou mudança de emprego.....	19
12- Segurança Física e Ambiental.....	19
13- Segurança Vinculada a Ativos.....	19
13.1 Inventário de Ativos.....	19
13.2 Controle de estoque.....	20
13.3 Propriedade de ativos.....	20
13.4 Uso aceitável de ativos.....	21
13.5 Classificação das informações.....	21

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	3 / 35

13.6 Tratamento de disco rígido obsoleto.	22
13.7 Tratamento para licenças de pessoal.	23
13.8 Política de controle e prevenção de perda ou vazamento de informações.....	24
14- Gerenciamento de Incidentes.....	25
15- Detecção de vulnerabilidade.....	26
15.1 Realize testes de detecção de vulnerabilidades.....	26
15.2 Categoria de Vulnerabilidade.....	26
15.3 Identificar e validar vulnerabilidades analisando fontes de monitoramento.....	27
15.4 Classifique a vulnerabilidade.....	27
15.5 Analise e documente a vulnerabilidade.....	28
15.6 Definir o plano de ação.....	28
15.7 Implementar alterações ou relatar.....	28
15.8 Monitorar o plano de ação.....	29
15.9 Ferramentas autorizadas para testes de vulnerabilidade.....	29
15.10 Política de “PenTesting”	29
16- Treinamento.....	30
17- Critérios para uso de criptografia.....	30
17.1 Desenvolvimento de Políticas.....	30
17.2 Separação de uso de chaves.....	31
17.3 Principais períodos de duração.....	31
17.4 Principais procedimentos de gestão.....	32
17.5 Conformidade regulatória.....	33
17.6 Funções e responsabilidades em relação à criptografia.....	33
17.7 Criação, modificação e atualização.....	33
18- Procedimentos básicos de instalação: Rede, Notebook e Servidores.	33
18.1- Rede.....	34
18.2- Notebook.....	34
18.3- Servidores.....	34

1. introdução

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	4 / 35

Ativos de informação e equipamentos de informática são recursos importantes e vitais da nossa Empresa.

Sem eles estaríamos rapidamente fora do mercado e por esta razão a Direção e a Assembleia têm o dever de preservá-los, utilizá-los e melhorá-los. Isto significa que devem ser tomadas medidas adequadas para garantir que a informação e os sistemas informáticos estão devidamente protegidos contra muitos tipos de ameaças e riscos, tais como fraude, sabotagem, espionagem industrial, extorsão, violação da privacidade, intrusos, hackers, interrupção de serviço, acidentes e desastres naturais.

As informações pertencentes à Empresa devem ser protegidas de acordo com seu valor e importância. As medidas de segurança devem ser utilizadas independentemente da forma como a informação é armazenada (em papel ou eletrônica), ou processada (PC, servidores, correio de voz etc.), ou transmitida (e-mail, conversa telefônica).

Essa proteção inclui restrições de acesso aos usuários de acordo com sua posição. As diferentes administrações da Empresa têm o dever e a responsabilidade de dedicar tempo e recursos suficientes para garantir que os ativos de informação estejam suficientemente protegidos.

Quando ocorre um incidente grave que reflete uma fraqueza nos sistemas informáticos, devem ser tomadas ações corretivas rapidamente para reduzir os riscos. Em qualquer caso, será realizada anualmente uma análise de risco e a revisão das políticas de segurança.

Da mesma forma, será elaborado anualmente um relatório para a Direção Geral que mostra o estado atual da Empresa em termos de segurança informática e os progressos alcançados.

Todos os Colaboradores devem receber formação, informação e avisos para que possam proteger e gerir adequadamente os recursos informáticos da Empresa.

Ressalta-se que a segurança informática é uma atividade tão vital para a Empresa quanto a contabilidade e a folha de pagamento.

O objetivo das políticas de segurança descritas abaixo é fornecer instruções específicas sobre como manter mais seguros os computadores da Empresa (em rede ou não) e as informações neles armazenadas. A violação destas políticas pode resultar em ação disciplinar, incluindo demissão.

Gerente General Grupo Inngen

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	5 / 35

2- Responsabilidades

As seguintes entidades são responsáveis, em diferentes graus, pela segurança na Empresa:

- A Comissão de Segurança Informática é composta por representantes dos diferentes departamentos da Empresa, bem como pelo Gestor Informático e pelo advogado ou representante legal da Empresa. Este Comitê é responsável por desenvolver e atualizar políticas, padrões, diretrizes e procedimentos relacionados à segurança informática. É também responsável pela coordenação da análise de riscos, planos de contingência e prevenção de desastres. Durante as suas reuniões trimestrais, a Comissão avaliará e analisará a situação da Empresa em termos de segurança informática, incluindo a análise dos incidentes ocorridos e que afetem a segurança.
- A Gestão de TI é responsável por implementar e garantir o cumprimento das políticas, padrões, diretrizes e procedimentos de segurança em toda a organização, tudo em coordenação com a Direção Geral. É também responsável por avaliar, adquirir e implementar produtos de segurança informática, e realizar outras atividades necessárias para garantir um ambiente informático seguro. Além disso, deve prestar apoio técnico e administrativo em todas as questões relacionadas com a segurança e, em particular, em casos de infecção por vírus, penetração de hackers, fraude e outros contratemplos.
- O Diretor de Segurança é responsável por dirigir investigações sobre incidentes e questões relacionadas à segurança, bem como recomendar ações apropriadas.
- O Administrador de Sistemas é responsável por estabelecer controles de acesso apropriados para cada usuário, supervisionar o uso dos recursos do computador, revisar os logs de acesso e realizar tarefas de segurança relacionadas aos sistemas que gerencia, como, aplicar imediatamente patches corretivos quando receber notificação do fabricante do produto. O Administrador de Sistemas também é responsável por relatar qualquer atividade suspeita ou evento incomum ao Chefe de Segurança e seus superiores. Quando não houver Diretor de Segurança, o Administrador de Sistemas exercerá as suas funções.
- Os utilizadores são responsáveis pelo cumprimento de todas as políticas da Empresa relacionadas com a segurança informática e, em particular:
 - Conhecer e aplicar as políticas e procedimentos adequados em relação à gestão da informação e dos sistemas informáticos.
 - Não divulgue informações confidenciais da Empresa a pessoas não autorizadas.
 - Não permita e não facilite o uso dos sistemas informáticos da Empresa a pessoas não autorizadas.
 - Não utilizar recursos de informática (hardware, software ou dados) e de telecomunicações (telefone, fax) para outras atividades que não estejam diretamente relacionadas ao trabalho na Empresa.
 - Proteja cuidadosamente a sua senha e evite que ela seja vista inadvertidamente por outras pessoas.
 - Selecione uma senha forte que não tenha nenhuma relação óbvia com o usuário, seus familiares, o grupo de trabalho e outras associações semelhantes.
 - Comunicar imediatamente ao seu chefe imediato ou a um responsável pela Segurança Informática qualquer evento que possa comprometer a segurança da Empresa e dos seus recursos informáticos, tais como propagação de vírus, intrusos, modificação ou perda de dados e outras atividades incomuns.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	6 / 35

3- Compromisso de Gestão

A Alta Direção da Organização declara estar comprometida com a informação, como um de seus ativos mais importantes, portanto, expressa seu total comprometimento com o estabelecimento, implementação e gestão de um Sistema de Segurança da Informação que inclua o desenho e implementação de um sistema de continuidade e desastres. plano de recuperação. A Alta Administração demonstrará seu comprometimento através de:

- A revisão e aprovação da política contida neste documento.
- Divulgação desta política a todos os dirigentes da Empresa.

Garantir recursos adequados para implementar e manter a política de Segurança da Informação.

4- Políticas de segurança informática

- Os computadores da empresa só devem ser usados em um ambiente seguro. Um ambiente é considerado seguro quando medidas de controle apropriadas foram implementadas para proteger software, hardware e dados. Estas medidas devem estar de acordo com a importância dos dados e a natureza dos riscos previsíveis.
- Os equipamentos da empresa devem ser utilizados apenas para atividades laborais e não para outros fins, como jogos e hobbies.
- A configuração de hardware e software estabelecida pelo Departamento de TI deverá ser respeitada e não modificada.
- Não é permitido fumar, comer ou beber durante a utilização de um PC.
- O equipamento deve ser protegido contra riscos ambientais (por exemplo, poeira, fogo e água).
- Devem ser utilizados protetores contra picos de energia elétrica e fontes de alimentação interrompíveis nos servidores.
- Qualquer falha no computador ou na rede deve ser comunicada imediatamente, pois pode causar problemas graves, como perda de informações ou indisponibilidade de serviços.
- O equipamento deve ser protegido para reduzir o risco de roubo, destruição e uso indevido. As medidas recomendadas incluem o uso de guardas de segurança e fechadura com chave.
- Os equipamentos devem ser marcados para identificação e controle de estoque. Os registros de estoque devem ser mantidos atualizados.
- O equipamento não pode ser movido ou realocado sem permissão. É necessária autorização por escrito para levar equipamentos para fora da Empresa.
 - A perda ou roubo de qualquer componente de hardware ou programa de software deve ser comunicada imediatamente.
- Para evitar acesso não autorizado, os usuários devem usar um sistema de senha robusto e também configurar o protetor de tela para ativar após 15 minutos de inatividade e exigir uma senha ao retomar a atividade. Além disso, o usuário deve ativar o protetor de tela manualmente sempre que estiver fora do escritório.
- Se um PC tiver acesso a dados confidenciais, deverá possuir um mecanismo especial de controle de acesso, de preferência hardware.
- Os dados confidenciais exibidos na tela devem ser protegidos contra visualização por terceiros através da disposição adequada de móveis de escritório e protetores de tela. Quando não forem mais necessários ou úteis, os dados confidenciais deverão ser excluídos.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	7 / 35

- Um sistema de autorização e controle de acesso deve ser implementado para restringir a capacidade dos usuários de ler, escrever, modificar, criar ou excluir dados importantes. Esses privilégios devem ser definidos de maneira consistente com as funções que cada usuário desempenha.
- Não é permitido trazer computadores portáteis (laptops) para o local de trabalho e, se necessário, deverá ser solicitada a autorização correspondente.
- Para evitar a intrusão de hackers através de backdoors, não é permitida a utilização de modems em PCs que também possuam conexão à rede local. (LAN), a menos que devidamente autorizado. Todas as comunicações de dados devem ser realizadas através da LAN da Empresa.
- Salvo indicação em contrário, os usuários devem presumir que todo o software da Empresa é protegido por direitos autorais e requer uma licença para uso. Por este motivo, é ilegal e estritamente proibido fazer cópias ou utilizar este software para fins pessoais.
- Os usuários não devem copiar software ou dados residentes nos computadores da Empresa para mídia removível (como um pendrive) sem aprovação prévia da administração.
- Os dados não podem ser extraídos fora da sede da Empresa sem aprovação prévia da administração. Esta política é particularmente relevante para aqueles que utilizam computadores portáteis ou estão ligados a redes como a Internet.
- Uma ferramenta antivírus deve ser instalada, ativada e mantida atualizada. Caso seja detectada a presença de um vírus ou outro agente potencialmente perigoso, o Chefe de Segurança da Informação deverá ser imediatamente notificado e o PC colocado em quarentena até que o problema seja resolvido.
- Os arquivos só podem ser baixados de redes externas de acordo com procedimentos estabelecidos. Um programa antivírus deve ser utilizado para examinar todos os softwares provenientes de fora ou mesmo de outros departamentos da Empresa.
- Software baixado da Internet e, em geral, software proveniente de fonte não confiável não deve ser utilizado, a menos que tenha sido rigorosamente testado e seu uso seja aprovado pelo Departamento de TI.
- Para evitar reclamações legais ou a introdução de vírus informáticos, é estritamente proibida a instalação de software não autorizado, incluindo aquele que tenha sido adquirido pelo utilizador. Da mesma forma, não é permitida a utilização de software distribuído gratuitamente ou shareware, a menos que tenha sido previamente aprovado pelo Departamento de Informática.
- Para ajudar a restaurar programas originais, não danificados ou infectados, cópias de todos os novos softwares devem ser feitas antes do uso e essas cópias devem ser armazenadas em um local seguro.
- Pendrives ou outros meios de armazenamento não devem ser utilizados em nenhum computador da Empresa, a menos que tenham sido previamente verificados como livres de vírus ou outros agentes nocivos.
- Os dados armazenados em PCs e servidores devem ser submetidos a backups periódicos e as cópias de backup devem ser mantidas em um local seguro e à prova de intempéries. roubo, incêndio e inundações. Programas e dados vitais para o funcionamento da Empresa deverão ser armazenados em outro local, afastado do prédio.
- Os usuários de PC são responsáveis por proteger programas e dados contra perdas ou danos. Para sistemas multiusuário e sistemas de comunicação, o Administrador de cada um desses sistemas é responsável por fazer backups periódicos. Os gestores dos diferentes departamentos são responsáveis por definir quais informações devem ser salvas, bem como a frequência do backup (por exemplo: diário, semanal) e o método de backup (por exemplo: incremental, completo).
- As informações da empresa classificadas como confidenciais ou de uso restrito devem ser armazenadas e transmitidas de forma criptografada, utilizando ferramentas robustas de criptografia e aprovadas pela Gestão de TI.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	8 / 35

- As informações originais não criptografadas não devem ser excluídas até que seja comprovado que podem ser recuperadas dos arquivos criptografados através do processo de descriptografia.
- O acesso às chaves utilizadas para encriptação e desencriptação deverá ser estritamente limitado a pessoas autorizadas.
- Sempre que possível, as informações confidenciais devem ser removidas dos computadores e discos rígidos antes de serem enviados para reparo. Caso tal não seja possível, deve garantir-se que a reparação é efectuada por empresas responsáveis, com as quais foi assinado um contrato de confidencialidade. Alternativamente, o reparo deverá ser realizado sob a supervisão de um representante da Empresa.
- As impressoras não devem ser deixadas sem vigilância, especialmente se informações confidenciais da Empresa forem (ou forem) impressas.
- Os funcionários que usam um laptop que contém informações confidenciais da Empresa não devem deixá-lo sem vigilância, especialmente quando viajam, e essas informações também devem ser criptografadas.

5- Políticas de Segurança para comunicações

5.1 Propriedade da informação

Para melhorar a produtividade, a Empresa promove a utilização responsável das comunicações eletrônicas, nomeadamente telefone, correio de voz, e-mail e fax. Os sistemas de comunicação e as mensagens geradas e processadas por tais sistemas, incluindo cópias de segurança, devem ser consideradas propriedade da Empresa e não propriedade dos utilizadores dos serviços de comunicação.

5.2 Uso de sistemas de comunicação

- Os sistemas de comunicação da Empresa geralmente devem ser usados apenas para atividades de trabalho. O uso pessoal ocasional é permitido desde que consuma um mínimo de tempo e recursos e não interfira na produtividade do Colaborador ou nas atividades da Empresa.
- É proibida a utilização de sistemas de comunicação para atividades comerciais privadas ou para fins de entretenimento e diversão.
- A navegação na Internet para fins pessoais não deve ser feita à custa do tempo e dos recursos da Empresa e os horários não laborais devem ser utilizados neste sentido.

5.3 Confidencialidade e privacidade

- Os recursos, serviços e conectividade disponíveis através da Internet abrem novas oportunidades, mas também introduzem novos riscos. Em particular, as mensagens que contenham informações confidenciais não devem ser enviadas pela Internet, a menos que sejam encriptadas. Para tanto deverão ser utilizados PGP, Outlook ou outros produtos previamente aprovados pela Gerência de TI.
- Colaboradores e dirigentes da Empresa não devem interceptar comunicações ou divulgar seu conteúdo. Nem deveriam ajudar outros a fazê-lo. A Empresa está comprometida em respeitar os direitos dos seus Colaboradores, incluindo a sua privacidade. É também responsável pelo bom funcionamento e utilização adequada das suas redes de comunicação e para isso é ocasionalmente necessário interceptar determinadas comunicações.
- É política da Empresa não monitorar regularmente as comunicações. No entanto, o uso e o conteúdo das comunicações podem ocasionalmente ser

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	9 / 35

supervisionado, se necessário, para atividades de manutenção, segurança ou auditoria. Pode acontecer que a equipe técnica visualize o conteúdo de uma mensagem de um Colaborador individual durante a resolução de um problema.

- De maneira consistente com as práticas geralmente aceitas, a Empresa processa dados estatísticos sobre o uso de sistemas de comunicação. Por exemplo, os relatórios da central telefônica contêm detalhes sobre o número chamado, a duração da chamada e a hora em que a chamada foi feita.

5.4 Encaminhamento de mensagens

Tendo em conta que determinadas informações são direcionadas a pessoas específicas e podem não ser adequadas a outras, dentro e fora da Empresa, alguns cuidados devem ser tomados no envio de mensagens. Em qualquer caso, informações confidenciais da Empresa não deverão ser enviadas sem a devida aprovação.

5.5 Excluindo mensagens

As mensagens que não são mais necessárias devem ser excluídas periodicamente de sua área de armazenamento. Isso reduz o risco de outras pessoas acessarem essas informações e também libera espaço em disco.

6- Política de Privacidade para redes

6.1 Propósito

o propósito de esta política É estabelecer as diretrizes, os procedimentos e os requisitos para assegurar a proteção apropriada da Companhia quando estiver conectada a redes de computadores.

6.2 Escopo

A Política de Segurança da Informação aplica-se a todos os níveis do Grupo Inngen: utilizadores (que inclui funcionários e clientes) e entidades que controlam, interna ou externamente, qualquer ativo de informação independentemente da sua localização. Além disso, esta Política se aplica a todas as informações criadas, processadas ou utilizados a nível corporativo, independentemente do meio, formato, apresentação ou local em que se encontrem.

6.3 Aspectos gerais

É política da Empresa proibir a divulgação, duplicação, modificação, destruição, perda, uso indevido, roubo e acesso não autorizado de informações proprietárias. Além disso, é sua política proteger as informações que pertencem a outras empresas ou indivíduos e que lhe foram confiadas.

6.4 Modificações

Todas as alterações na central telefônica e nos servidores e equipamentos de rede da Empresa, incluindo a instalação de novos softwares, a alteração de endereços IP, a reconfiguração de routers e switches, deverão ser documentadas e devidamente aprovadas, exceto se se tratar de uma situação de emergência. Tudo isso

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	10 / 35

para evitar problemas por mudanças precipitadas que podem causar interrupção das comunicações, interrupção da rede, negação de serviço ou acesso inadvertido a informações confidenciais.

6.5 Contas de usuário

- Quando um usuário recebe uma nova conta, deverá assinar um documento declarando que está ciente das políticas e procedimentos de segurança e aceita suas responsabilidades em relação ao uso dessa conta.
- O pedido de nova conta ou alteração de privilégios deverá ser feito por escrito e devidamente aprovado.
- Uma conta não deverá ser concedida a pessoas que não sejam Associados da Empresa, a menos que estejam devidamente autorizados, caso em que a conta deverá expirar automaticamente após um período de 30 dias.
 - Privilégios especiais, como a capacidade de modificar ou excluir arquivos de outros usuários, só devem ser concedidos aos responsáveis diretos pela administração ou segurança dos sistemas.
- Os técnicos de manutenção não devem receber contas ou acesso remoto, a menos que o administrador de sistemas ou gerente de TI determine que seja necessário. Em qualquer caso, esta facilidade só deve ser habilitada durante o período de tempo necessário para a realização do trabalho (como manutenção remota). Se for necessária uma conexão remota por um período mais longo, deverá ser utilizado um sistema de autenticação mais robusto baseado em senhas dinâmicas, tokens ou cartões inteligentes.
- É proibido o uso de contas anônimas ou de convidados e os usuários deverão entrar no sistema através de contas que indiquem claramente sua identidade. Isso também significa que os administradores do sistema não devem fazer login inicialmente como root, mas primeiro usar seu próprio ID e depois usar "set userid" para obter acesso root. Em qualquer caso, todas as alterações de ID devem ser registradas no log.
- Qualquer conta é automaticamente suspensa após um certo período de inatividade. O período recomendado é de 30 dias.
- Os privilégios de sistema concedidos aos usuários devem ser ratificados a cada 6 meses. O Administrador de Sistemas deve revogar imediatamente a conta ou privilégios de um usuário ao receber uma ordem de um superior e, em particular, quando um Colaborador deixa de funcionar.
- Quando um Colaborador é demitido ou pede demissão da Empresa, sua conta deverá ser desativada antes de deixar o cargo. Senhas e controle de acesso.
 - O usuário não deve salvar sua senha de forma legível em arquivos em disco, nem escrevê-la em papel e deixá-la em locais onde possa ser encontrada. Se houver motivos para acreditar que uma senha foi comprometida, você deverá alterá-la imediatamente. Senhas idênticas ou substancialmente semelhantes às senhas usadas anteriormente não devem ser usadas. Sempre que possível, os utilizadores devem ser impedidos de reutilizar palavras-passe anteriores.
- A senha nunca deve ser compartilhada ou revelada a terceiros. Fazer isso expõe o usuário às consequências das ações que outras pessoas realizam com essa senha.
- É proibido o uso de senhas de grupo para facilitar o acesso a arquivos, aplicativos, bancos de dados, computadores, redes e outros recursos do sistema. Isto se aplica especialmente à senha do administrador.
 - As senhas iniciais emitidas para um novo usuário devem ser válidas apenas para a primeira sessão. Nesse momento, o usuário deverá escolher outra senha.
- As senhas predefinidas que acompanham os novos equipamentos, como roteadores, switches, etc., devem ser alteradas imediatamente quando o equipamento for colocado em serviço.
- Para evitar ataques, quando o software do sistema permitir, o número de tentativas consecutivas sem sucesso de inserir a senha deve ser limitado a 3, após o qual a conta envolvida é suspensa e o Administrador do Sistema é alertado. Caso seja acesso remoto via modem dial-up, a sessão deverá ser imediatamente desconectada.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	11 / 35

- Para acesso remoto aos recursos computacionais da Companhia, a combinação do ID do usuário e uma senha fixa não oferece segurança suficiente, portanto é recomendada a utilização de um sistema de autenticação mais robusto baseado em senhas dinâmicas, tokens ou cartões inteligentes.
- Se não houver atividade em um terminal, PC ou estação de trabalho por um determinado período de tempo, o sistema deverá limpar automaticamente a tela e suspender a sessão. O período de tempo recomendado é de 15 minutos. O restabelecimento da sessão exige que o usuário forneça autenticação usando sua senha (ou use outro mecanismo, por exemplo, cartão inteligente ou de proximidade).
- Se o sistema de controle de acesso não estiver funcionando corretamente, você deverá negar o acesso do usuário até que o problema seja resolvido.
- Os usuários não devem tentar violar sistemas de segurança e controle de acesso. Ações desta natureza são consideradas violação das políticas da Empresa e podem ser motivo de demissão.
- Para fornecer provas em casos de ações disciplinares e judiciais, determinados tipos de informações devem ser capturados, registrados e salvos quando há suspeita de abuso, fraude ou outros crimes envolvendo sistemas informáticos.
- Os arquivos de log e trilhas de auditoria que registram eventos relevantes relativos à segurança dos sistemas informáticos e das comunicações devem ser revisados periodicamente e mantidos por um período razoável de pelo menos três meses. Esses arquivos são importantes para detecção de invasões, violações de segurança, investigações e outras atividades de auditoria. Por isso, devem ser protegidos para que ninguém possa alterá-los e que apenas pessoas autorizadas possam lê-los.
- Os servidores de rede e os equipamentos de comunicação devem estar localizados em locais apropriados, protegidos contra danos e roubo. O acesso a essas instalações e salas de fiação por parte de pessoas não autorizadas deve ser severamente restringido através do uso de fechaduras e outros sistemas de acesso.

7- Gestão de Segurança da Informação

7.1 Objetivos Gerais

O objetivo geral do sistema de gestão de segurança da informação é proteger os ativos de informação que são utilizados no serviços, buscando criar um quadro de confiança para as partes interessadas, controlando a confidencialidade, integridade e disponibilidade, gerenciando riscos, reduzindo incidentes, treinando pessoal nos conceitos de segurança da informação e no sistema de gestão de segurança, tudo enquadrado num processo de melhoria contínua.

7.2 Objetivos específicos

- Desenhar e implementar controles relacionados com a disponibilidade, confidencialidade e integridade do serviço de Faturação Eletrônica - Viável
- Identificar, avaliar e controlar os riscos associados à perda de confidencialidade, integridade e disponibilidade da informação do serviço de Faturação Eletrônica - Viável
- Definir os controles para a gestão de incidentes de segurança da informação do serviços, para garantir a melhoria contínua do sistema de gestão da segurança da informação.
- Estabelecer mecanismos para estimular a cultura organizacional dos funcionários do Grupo Inngen responsáveis pelo serviços, na área de segurança da informação.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	12 / 35

7.3 Medição de Objetivos

A Autoridade de Privacidade de Dados da informação é responsável por medir o cumprimento dos objetivos; A medição será realizada pelo menos uma vez por ano e o Diretor de Segurança da Informação analisará e avaliará os resultados e reportá-los-á à Alta Administração como material para sua revisão.

No mínimo, avaliará as seguintes medidas que estão relacionadas com os objectivos específicos acima definidos.

- Número de controles que foram projetados e implementados
- Dos riscos identificados e avaliados, quantos dos riscos que requerem tratamento foram efetivamente tratados com um controle.
- Durante a operação do serviço são medidos o número de incidentes mensais e as medidas corretivas implementadas a eles associadas.
- Medir a proporção entre o número de colaboradores envolvidos com o serviço de Faturação Eletrônica – Viável e os que frequentam a formação realizada.

7.4 Requisitos para Segurança da Informação

Esta Política, e todo o Sistema de Gestão de Segurança da Informação (SGSI), devem cumprir os requisitos legais e regulamentares importantes para o Grupo Inngen no domínio da segurança da informação relacionados com o serviços.

8- Política de Segurança Específica

A seguir, são desenvolvidas políticas específicas diretamente associadas aos domínios, objetivos de controle e controles, diretamente relacionados à Política Geral, que especificam a conduta aceita pelo Grupo Inngen na gestão de sua informação e as ações que devem ser tomadas para atingir os objetivos. esta política.

8.1 Segregação de deveres

Controle: Deveres e áreas de responsabilidade conflitantes devem ser separados para reduzir as possibilidades de modificação não autorizada ou não intencional de informações ou uso indevido de ativos organizacionais.

8.2 Contato com autoridades

Controle: Devem ser mantidos contatos apropriados com as autoridades competentes, que podem ajudar a resolver conflitos relativos à segurança da informação.

8.3 Segurança da informação na gestão de projetos

Controle: Durante o planejamento e execução dos projetos Grupo INNGEN, além das áreas interessadas, a área de Segurança da Informação deverá participar como geradora de recomendações na avaliação dos riscos inerentes aos referidos projetos.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	13 / 35

8.4 Política de controle de acesso

Controle: O uso das informações do Grupo Inngen deve ser controlado para evitar acesso não autorizado. Os privilégios de informação devem ser concedidos e mantidos de acordo com as necessidades da operação, limitando o acesso apenas ao que é necessário.

8.5 Controle de acesso a redes e serviços associados

Controle: O acesso à rede Grupo Inngen deverá ser concedido apenas a utilizadores autorizados, prévia definição, verificação e controlo dos perfis e funções de acesso nos diferentes sistemas de informação, em coordenação com a área de Recursos Humanos, a Direção Administrativa e a Direção de TI.

8.6 Solicitação de acesso.

Na computação, um acesso é o resultado positivo de uma autenticação; o acesso pode durar muito tempo ou momentaneamente. Para garantir e controlar o acesso é necessário seguir as seguintes orientações:

Fases:

- Aplicativo
- Aprovação
- Acesso
- Revisão
- Remoção

Solicitações:

Todas as solicitações devem ser gerenciadas a partir da plataforma Internal Ticket Management-Access Request.

A solicitação deverá conter detalhadamente os seguintes aspectos: Motivo ou Necessidade, Data de Início, Duração, tipo de acesso e ações a serem realizadas.

Caso não tenha acesso à plataforma, deverá entrar em contato com o RH que poderá gerenciar a solicitação.

Aprovação:

A solicitação deverá ser analisada pelo Gerente Geral; isto pode ser Aprovado ou Rejeitado Parcial ou Definitivamente.

Podem ocorrer rejeições parciais caso o Gestor exija mais detalhes ou o prazo não corresponda à solicitação.

Acesso:

Uma vez aprovada a solicitação, o Gerente Geral (no caso de Ambiente ou Servidores AWS) ou o Gerente de TI (Rede, equipamentos ou outros) são responsáveis por conceder o acesso gerenciado em conformidade com o respectivo nível de permissões.

Revisão:

A revisão dos acessos deverá ser realizada obrigatoriamente a cada 3 meses. Isso deve ser realizado pelo Gerente de TI.

Se você encontrar acesso não autorizado ou expirado, deverá reportá-lo ao Gerente Geral antes de remover as licenças.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	14 / 35

Remoção ou Suspensão:

A remoção deverá ser realizada pelo Gerente Geral (no caso de Ambiente ou Servidores AWS) ou Gerente de TI (Rede, equipamentos ou outros).

- Suspender o acesso a contas inativas por mais de 180 dias. *
- Remover acesso de contas inativas há mais de 365 dias. *
- Remova o acesso indocumentado. **
- Remover o acesso dos perfis de teste ou treinamento ao final da data indicada. **

*Esta política será controlada pelo Gerente de TI, através de alertas automáticos desenvolvidos pela empresa. O gestor em questão receberá por email relatórios de todas as contas detalhadas no prazo indicado para que possa proceder à Inativação ou Eliminação do acesso.

**Esta política será controlada pelo Gerente de TI (consulte a seção 8.6 Revisão)

8.7 Identificação do Perfil.

Os perfis deverão ter a seguinte identificação: PRIMEIRO.SOBRENOME

O nome e o sobrenome devem corresponder aos registros de RH para facilitar a identificação em caso de auditoria.

8.8 Novos acessos.

Para novos funcionários que devam desempenhar funções que exijam acesso à rede ou a sistemas informáticos.

Equipes:

- O acesso é concedido pela equipe de TI.
- A identificação do utilizador deverá ser gerada respeitando o ponto de identificação dos Perfis (ver ponto 8.7).
- A senha inicial deverá ser modificada pelo usuário no primeiro login. Esta alteração é obrigatória para poder retirar o equipamento do departamento de TI. ***

Plataforma de Gestão:

- O acesso é concedido pelo RH
- A identificação do utilizador deverá ser gerada respeitando o ponto de identificação dos Perfis (ver ponto 8.7).
- A senha inicial deverá ser modificada pelo usuário no primeiro login. Isso deve ser feito ao mesmo tempo em que a credencial é concedida na presença do pessoal de RH. ***

***O código de acesso é gerado automaticamente e enviado via SMS para o dispositivo pessoal do utilizador, isto é conseguido através da gestão de notificações/alertas desenvolvidas pela empresa.

A senha será gerada novamente a cada 4 horas desde que o usuário não a acesse e altere. A partir do terceiro alerta emitido (12 horas após a primeira notificação) o Gestor de TI será notificado para entrar em contato com o usuário ou reiniciar o procedimento.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	15 / 35

8.9 Revisão de Atividades (logs).

Ter logs permite realizar investigações especiais, cumprir regulamentos, verificar eventos de segurança, entre outros.

É responsabilidade da TI estar atenta à ativação dos logs de auditoria de todas as aplicações da empresa.

Verificação de evento:

Registros sobre atividades de usuários, exceções, falhas e eventos de segurança da informação devem ser criados, mantidos e revisados periodicamente.

É responsabilidade de cada área solicitar e saber quais eventos ocorreram em seus sistemas de processamento de informações.

É responsabilidade do departamento de TI fornecer as informações do evento solicitadas pelas respectivas áreas.

Acesso aos registros:

As solicitações deverão ser enviadas via e-mail para o departamento de TI (suporte@iwsdinnero.com). Você tem acesso aos diversos aplicativos para geração de relatórios.

Os laudos deverão ser solicitados pelas áreas com 3 dias de antecedência. Salvo situações excepcionais que comprometam ou envolvam a segurança ou as atividades da empresa.

9- Procedimentos e políticas específicas

9.1 Política de dispositivos móveis

O utilizador de equipamentos informáticos e telefónicos móveis deve cumprir determinadas regras quando transporta os seus equipamentos para fora das instalações da entidade, nomeadamente no que diz respeito a:

- O usuário deve tentar não deixar seus equipamentos de informática e telefonia móvel sem vigilância.
- O usuário deve garantir que seu trabalho não fique visível para outras pessoas que estejam próximas.
- O usuário deve procurar manter seus equipamentos de informática e telefonia móvel atualizados e com os mais recentes patches de segurança.
- O usuário deve tentar manter seus antivírus e softwares de controle de códigos maliciosos atualizados.
- O usuário é responsável por fazer cópias de segurança dos dados.
- O usuário deve verificar se a conexão com um serviço web é segura.

9.2 Política de Utilização Aceitável

O Grupo Inngen definiu uma política de uso aceitável para funcionários:

- Responsabilidade pelos ativos e seu inventário.
- Atividades proibidas.
- Devolução de bens no final do contrato.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	16 / 35

- Procedimento para cópias de segurança.
- Proteção antivírus.
- Autorização para utilização de sistemas de informação.
- Responsabilidades da conta do usuário.
- Responsabilidades pela chave ou senha.
- Utilização de impressoras, scanners e fotocopiadoras.
- Uso da Internet.
- E-mail, mensagens de texto e redes sociais.
- Direitos autorais.
- Uso de armazenamento externo.

Este documento estará disponível para leitura do usuário ou funcionário vinculado ao serviços.

9.3 Política de Classificação de Informações

O grupo INNGEN definiu para os colaboradores vinculados ao serviços que as informações sejam classificadas em três níveis:

1. Pública: A informação está disponível ao público.
2. Confidencial: As informações estão disponíveis para todos os funcionários e alguns terceiros selecionados, portanto não podem ser compartilhadas com o público em geral.
3. Segreda: As informações estão disponíveis para alguns funcionários específicos, portanto eles não poderão compartilhá-las com mais ninguém.

As informações confidenciais e secretas deverão ser acompanhadas de uma marca que identifique a sua classificação, as demais informações serão automaticamente classificadas como públicas, possuam ou não a marca correspondente.

Todas as pessoas que tenham acesso a informações confidenciais e secretas devem seguir as regras especificadas no documento Política de Classificação de Informações.

9.4 Política de Transferência de Informações

As informações do Grupo Inngen para colaboradores relacionadas aos serviços poderão ser trocadas por meio dos seguintes canais de comunicação eletrônica: e-mail, sistemas de armazenamento em nuvem e sistemas de transferência web. A forma de transferência e o uso da criptografia dependerão da classificação de cada ativo de informação a ser transferido.

9.5 Procedimento para trabalho em área segura

A entrada de pessoal nas áreas seguras é restrita, somente terão acesso os funcionários vinculados ao serviços, conforme estabelecido na Política de Controle de Acesso.

Os visitantes deverão ser sempre acompanhados por um dos funcionários com acesso.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	17 / 35

10- Criptografia

10.1 Controles criptográficos.

Objetivo: O objetivo é garantir o uso adequado e eficaz da criptografia para proteger a confidencialidade, autenticidade e/ou integridade das informações.

10.2 Política de uso de controles criptográficos

Controle: O GRUPO INNGEN garantirá que as informações, classificadas como reservadas ou restritas, serão criptografadas no momento do armazenamento e/ou transmissão por qualquer meio, com a finalidade de proteger sua confidencialidade e integridade.

10.3 Gerenciamento de chaves

Controle: O GRUPO INNGEN deve proteger os tipos de chave contra modificação ou destruição; As chaves secretas e privadas também requerem proteção contra distribuição não autorizada. Para tanto, técnicas de criptograma devem ser utilizadas para garantir a confiabilidade das informações. A proteção física deve ser usada para cobrir equipamentos usados na geração, armazenamento e arquivamento de chaves.

10.4 Formato chave:

Para proteger informações próprias ou de terceiros, as senhas devem ser seguras. Uma senha forte deve ter a seguinte combinação:

- Números
- Cartas
- Maiúsculas e Minúsculas.
- Caracteres especial.
- Mínimo 8 dígitos.
- Os últimos 12 anteriores não podem ser utilizados.
- Validade da chave: 90 dias.
- Evite alterações mais de 4 vezes ao dia.
- Validade mínima da senha 7 dias. *

*Evitar alterações de senha fora dos prazos permite controlar e evitar o uso inadequado de sistemas ou equipamentos.

Caso o usuário solicite a alteração fora dos prazos, deverá gerenciá-la e justificá-la na plataforma de tickets.

10.5 Criptografia de chave:

As chaves em repouso devem ser protegidas de maneira segura para evitar acesso não autorizado. A criptografia que deve ser utilizada deve garantir uma segurança robusta, por isso deve ter as seguintes características:

- Modo de cifrado HASH

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	18 / 35

- Método de cifrado Bcrypt.

11- Segurança Ligada aos Recursos Humanos

11.1 Antes de contratar:

Objetivo: garantir que os Colaboradores e contratados entendam suas responsabilidades e sejam adequados para as funções para as quais são considerados.

11.2 Investigação de antecedentes

Controle: Novos Colaboradores que ingressem no Grupo INNGEN deverão passar por um processo de investigação de antecedentes, a fim de mitigar os riscos no uso da informação. Caso a investigação dê resultados adversos, o colaborador não é contratado.

11.3 Termos e condições do contrato

Controle: Os contratos dos colaboradores devem incluir cláusulas que especifiquem as responsabilidades e os cuidados que devem ter com as informações do Grupo Inngen.

11.4 Durante a contratação

Objetivo: Garantir que os Colaboradores e contratados estejam cientes e cumpram com suas responsabilidades de segurança da informação.

11.4 Responsabilidades de gestão

Controle: O GRUPO INNGEN deve fornecer os mecanismos necessários para garantir que os seus Colaboradores cumprem as suas responsabilidades de Segurança da Informação desde a sua entrada até à sua reforma.

11.5 Conscientização, educação e treinamento em segurança da informação

Controle: O GRUPO INNGEN deverá estabelecer um programa permanente de criação de cultura de segurança da informação para os Colaboradores, treinando-os constantemente em atualizações regulares sobre as políticas e procedimentos pertinentes ao seu cargo.

11.6 Processo disciplinar

Controle: As Políticas de Segurança da Informação com suas respectivas normas, padrões, procedimentos e demais documentos que são gerados e dão suporte ao Sistema de Gestão de Segurança da Informação são obrigatórias. A execução de ações que violem a confidencialidade, disponibilidade, integridade e privacidade de informações ou dados pessoais resultará em ação disciplinar que poderá estender-se à rescisão do contrato de trabalho e à eventual instauração de processo judicial nos termos da legislação nacional ou internacional aplicável.

11.7 Rescisão ou mudança de emprego

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	19 / 35

Controle: Os colaboradores ou contratantes devem ser informados das responsabilidades e deveres de segurança da informação que permanecem válidos após a rescisão ou alteração do contrato, os quais devem cumprir.

12- Segurança Física e Ambiental

Segurança de escritórios, escritórios e recursos

Controle: A entrada e saída de pessoal nas instalações do Grupo Inngen deverão ser devidamente registradas.

Proteção contra ameaças externas e ambientais:

Controle: O GRUPO INNGEN deverá fornecer as condições físicas e ambientais necessárias para certificar a proteção e o correto funcionamento dos recursos, especialmente da plataforma tecnológica localizada no centro de informática; Deverão existir sistemas de controlo ambiental de temperatura e humidade, sistemas de detecção e extinção de incêndios, sistemas de descargas eléctricas, sistemas de vigilância e monitorização e alarmes caso sejam detectadas condições ambientais inadequadas. Esses sistemas devem ser monitorados permanentemente.

Manutenção de Equipamento

Controle: Os meios e equipamentos onde a informação é armazenada, processada ou comunicada devem ser mantidos com medidas de proteção física e lógica que permitam a sua monitorização e correto estado de funcionamento; Para tanto, devem ser realizadas manutenções preventivas periodicamente semestralmente e manutenções corretivas quando necessárias.

Reutilização ou remoção segura de dispositivos de armazenamento

Controle: A área de Tecnologia deverá realizar a reutilização ou remoção segura dos dispositivos de armazenamento que contenham informações de DINHEIRO, por meio dos mecanismos necessários na plataforma tecnológica, seja quando houver cancelamento de registro ou mudança de usuário.

13- Segurança vinculada a ativos

13.1 Inventário de ativos:

O GRUPO INNGEN deve manter um inventário de recursos ou ativos de informação. Os proprietários das informações devem classificá-las com base em seu valor, sensibilidade, risco de perda ou comprometimento e/ou requisitos legais de retenção.

13.1.1 Periodicidade

Por volume de ativos, é estabelecido um inventário e monitoramento mensal como procedimento usual para se ter uma visão geral.

É estabelecido um inventário e controle semestral para contagem e revisão física dos bens para garantir a coincidência com os registros.

13.2 Controle de estoque:

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	20 / 35

É o processo pelo qual o jantar deve gerenciar os artefatos para maior controle e monitoramento deles.

a- Fases:

Aprovação

-Entrega

-Revisão

-Devolução ou Remoção.

-Solicitação

Todas as solicitações devem ser gerenciadas a partir da plataforma Internal Ticket Management-Teams.

A solicitação deverá conter detalhadamente os seguintes aspectos: Motivo ou Necessidade, Características e pelo menos dois orçamentos no caso de novas aquisições.

Caso não tenha acesso à plataforma, deverá entrar em contato com o RH que poderá gerenciar a solicitação.

b- Aprovação:

Dois níveis de aprovação:

Nível 1: Gerente da área. Este deve analisar a necessidade e garantir que o requisito atenda aos padrões da empresa.

Nível 2: Gestor de Ativos: Deve avaliar os ativos e verificar a viabilidade de novas aquisições.

c- Entrega:

A entrega deverá ser feita pelo Gerente de Área ou RH dependendo do caso. Deve ser documentado e assinado pelo requerente.

d- Revisão:

O Gestor de Ativos deverá realizar uma revisão obrigatória a cada 6 meses. Caso detecte desvios ou aspectos que não estejam de acordo com o padrão da empresa, deverá informar o Gerente de Área e o Gerente Geral.

e- Devolução ou Remoção:

A devolução deverá ser feita ao Gestor de Ativos; Um registro documentado deve ser deixado para cumprir ou facilitar o controle de estoque.

- Suspender o acesso a contas inativas por mais de 90 dias. *

- Remova o acesso de contas inativas há mais de 185 dias. *

*Esta política será controlada pelo Gestor de TI, através de alertas automáticos desenvolvidos pela empresa. O gestor em questão receberá por email relatórios de todas as contas detalhadas no prazo indicado para que possa proceder à Inativação ou Eliminação do acesso.

13.3 Propriedade de ativos

Controle: A área responsável pelo processo deverá realizar o devido controle e manutenção do inventário dos ativos de tecnologia e informação, para estabelecer a responsabilidade pela sua posse e pelas informações sobre eles, incluindo o controle do licenciamento de software.

13.4 Uso aceitável de ativos

Controle: independentemente do meio onde cada ativo informacional esteja localizado, eles devem ser classificados pelo proprietário da informação, utilizando o padrão de classificação estabelecido. Esses

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	21 / 35

controles devem ser aplicados e mantidos durante todo o ciclo de vida da informação, desde a sua criação, durante o seu uso autorizado e até a sua adequada disposição ou destruição.

13.5 Classificação da informação

Objetivo: garantir que a informação receba um nível adequado de proteção, proporcional à sua importância para a organização.

Nível 1. Informação pública: Os dados a este nível podem ser divulgados ao público em geral, sem qualquer implicação para o Grupo INNGEN. Os dados não são vitais. Perdas deste tipo de informação são de baixo risco e não requerem controles especiais. Por exemplo: informações de previsão e atualizações depois de aprovadas.

Nível 2. Informações Internas: As informações classificadas neste nível devem ser restritas ao acesso externo. Se for divulgado, as consequências são de risco médio. O acesso interno deve ser seletivo. A integridade das informações é importante, mas não vital. Neste nível é catalogado qualquer tipo de informação que possua pelo menos uma das seguintes características:

- Informações relevantes para processos, controles e registros internos.
- Manuais de responsabilidades organizacionais e de cargo.
- Informação operacional e técnica de sistemas de informação.

Nível 3. Informação confidencial. Este tipo de informação deve ser protegida de acessos externos e internos não autorizados. Se esta informação for do conhecimento de pessoas não autorizadas, existe o risco de afetar o normal funcionamento do Grupo Inngen, a sua reputação no mercado e a continuidade dos negócios. Neste nível é catalogado qualquer tipo de informação que possua pelo menos uma das seguintes características:

- Informação fornecida por outras entidades relacionadas com os seus clientes.
- Chaves de acesso associadas a serviços de consulta e modificação de informações do banco de dados.
- Código-fonte do aplicativo e informações técnicas confidenciais.
- Códigos de identificação e verificação do cliente.
- Códigos de acesso à conta.

13.5.2 Identificação da informação

a. Etiketado Manual: Os colaboradores ao criar ou gerenciar dados são responsáveis por rotulá-los de acordo com a política de classificação da organização. A etiquetagem deverá ser realizada através do sistema de tickets ao Gestor de TI com o assunto “etiqueta XXXX” e corpo “informação XXXX” + detalhe do suporte utilizado para salvaguarda da informação. Por exemplo, banco de dados XXX, arquivo XXX, pasta XXX, servidor XXX

b. Metadados: Todo documento criado com ferramentas Office (Word, PowerPoint) deverá possuir uma capa indicando a etiqueta de classificação das informações, nestes casos o Gestor de TI também deverá ser informado através do sistema de Tickets com referência ao servidor + localização + nome do arquivo na rede.

c. Banco de dados corporativo: Toda a informação armazenada nas bases de dados particulares e privadas dos clientes é classificada como “Nível 1. Informação confidencial”

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	22 / 35

d. Comunicações internas: Toda troca interna ou externa realizada através do sistema de tickets será considerada “Nível 2. Informações Internas”

13.5.3 Tempos de retenção

Nível 1: As informações públicas não têm restrições de tempo de retenção, salvo indicação em contrário por requisitos legais ou regulamentares.

Nível 2: As informações internas devem ser retidas por 5 anos a partir da data de criação ou recebimento, a menos que haja uma justificativa válida para mantê-las por um período mais longo.

Nível 3: As informações confidenciais devem ser retidas pelo tempo exigido pelas leis e regulamentos aplicáveis, bem como pelos requisitos operacionais. A retenção mínima será de 7 anos. Os prazos exatos serão determinados com base na natureza da informação e nos requisitos legais aplicáveis.

13.5.4 Política de exclusão

Nível 1: Como as informações públicas não contêm dados confidenciais, nenhum processo específico de exclusão é necessário. No entanto, a informação pública será revista e atualizada trimestralmente para garantir a sua precisão e relevância.

Nível 2: Ao final do período de retenção interna da informação, deve-se avaliar sua relevância e valor para a organização. Caso a retenção não seja necessária, o processo de exclusão segura deverá ser seguido de acordo com as diretrizes estabelecidas para informações confidenciais.

Nível 3: Depois que as informações confidenciais cumprirem seu período de retenção, um processo de exclusão seguro deverá ser seguido. Identifique o tipo de dispositivo onde a informação está armazenada, proceda à eliminação utilizando os diferentes métodos dependendo do tipo de armazenamento:

- Substituir: sobrescreve o dispositivo com informações aleatórias várias vezes para dificultar a recuperação.
- Apagamento físico: Seguindo as diretrizes da seção 13.6
- Dados criptografados: remova as chaves de criptografia para tornar os dados inacessíveis. Em seguida, aplique o procedimento de substituição.

13.5.4.1 Registro do procedimento de borrado

1. Escreva e envie para arquivo o documento de exclusão especificando a data, método utilizado e quaisquer informações relevantes para auditoria e conformidade regulatória.

13.5.4.2 Verificação de exclusão

2. Após a exclusão, será feita uma tentativa de recuperação dos dados para verificar se as informações desapareceram. Ferramenta para usar o Recuva.

13.6 Tratamento de disco rígido obsoleto.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	23 / 35

Os dados armazenados em discos rígidos podem conter informações relevantes ou confidenciais de clientes ou empresas.

Excluir os dados convencionalmente não é suficiente e não representa garantia de que não possam ser recuperados com uma ferramenta de restauração. As informações excluídas podem ser acessadas independentemente do modelo do disco.

A nossa empresa está empenhada em garantir a máxima confidencialidade dos dados, sejam eles empresariais ou de clientes.

Por esse motivo, estabelecemos as seguintes diretrizes que devem ser seguidas na íntegra:

Paso 1:

Formatação

Los discos obsoletos deben ser sometido a un formateo de bajo nivel, esto implica sobrescribir efectivamente la información eliminada. Este proceso debe repetirse mínimamente 2 veces.

Software autorizado para formatação de baixo nível:

1. CCleaner
2. Darik's Boot and Nuke (DBAN)

Paso 2:

Proteções

Os discos devem permanecer sob os cuidados do gerente de TI até serem destruídos. Com acesso restrito a eles.

Tempo máximo de armazenamento 6 meses.

*Sob nenhuma razão podem ser dados como presentes a funcionários da empresa ou terceiros.

Paso 3

Destruição

Os discos deverão ser enviados para empresas especializadas e certificadas em destruição total.

Empresa autorizada para destruição:

1. CBL Tech

13.7 Tratamento para licenças de funcionários.

Caso o funcionário solicite ausência por período superior a 30 dias, deverá ser seguido o seguinte procedimento:

Licenças entre 31 a 60 dias:

- Os funcionários deverão entregar os dispositivos fornecidos pela empresa como medida de segurança. Siga o procedimento: 13.2 -> C- Entrega

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	24 / 35

- O acesso do pessoal ao ecossistema Grupo Inngen deve permanecer bloqueado desde o primeiro dia da licença.

Aplica-se o procedimento: 13.2 -> E- Devolução ou Remoção.

Licenças superiores a 60 dias:

- Os funcionários deverão entregar os dispositivos fornecidos pela empresa como medida de segurança. Siga o procedimento: 13.2 -> C- Entrega

- O acesso do pessoal ao ecossistema Grupo Inngen deve ser eliminado.

Aplica-se o procedimento: 13.2 -> E- Devolução ou Remoção

Depois de decorrido o período de licença, a equipe deve gerenciar o processo de inscrição no RH. HH na plataforma Interna: Ticket-Team Management.

O procedimento se aplica: 13.2 na sua totalidade.

13.8 Política de controle e prevenção de perda ou vazamento de informações.

e. Objetivo

Garantir a proteção e confidencialidade das informações da organização, evitando o vazamento, distribuição ou divulgação não autorizada de dados através de meios eletrônicos como e-mail, chat, redes sociais e outros.

f. Alcance

Esta política se aplica a todos os funcionários, contratados, fornecedores e terceiros que tenham acesso aos sistemas e dados da organização.

g. Diretrizes Gerais

- Informações confidenciais ou protegidas não serão enviadas para fora da rede corporativa sem a devida autorização.
- Toda comunicação externa deverá ser realizada através das ferramentas disponibilizadas pela empresa.

h. Bate-papos e mensagens instantâneas

- É proibido compartilhar informações confidenciais ou protegidas através de plataformas de bate-papo não autorizadas.
- A organização optará por implementar soluções de mensagens criptografadas para comunicações internas ou externas.

i. Redes sociais

- É proibido o uso de sites não autorizados pela empresa.
- As contas oficiais de mídia social da organização devem ser gerenciadas por pessoal autorizado e treinado.

j. Medidas preventivas

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	25 / 35

- Controle de acesso: Serão implementados controles de acesso apropriados para garantir que apenas pessoal autorizado tenha acesso às informações. (Anexo DLP#1)
- Treinamento e Conscientização: Todos os funcionários devem receber treinamento regular sobre a importância da segurança da informação e como evitar vazamentos de dados. (Anexo DLP#2)
- Monitoramento: Devem existir sistemas para monitorar e alertar sobre qualquer atividade suspeita ou não autorizada.. (Anexo DLP#3)
- Revisión Regular: Auditorias e revisões periódicas das políticas e práticas de segurança devem ser realizadas. (Anexo DLP#4)

k. Relatórios de incidentes

Todos os funcionários devem reportar imediatamente qualquer atividade suspeita, violação ou vazamento de dados através dos canais estabelecidos pela organização.

l. Consequências do não cumprimento

O não cumprimento desta política pode resultar em ações disciplinares, que podem incluir advertências por escrito para demissão, bem como possíveis ações legais dependendo da gravidade do incidente.

m. Revise e atualize

Esta política será revisada y atualizada regularmente para reflejar los cambios en los requisitos legales, tecnológicos y del negocio.

14- Gerenciamento de Incidentes

O GRUPO INNGEN promoverá junto dos funcionários a comunicação de incidentes relacionados com a segurança da informação e dos seus meios de tratamento, incluindo qualquer tipo de suporte de armazenamento de informação, como a plataforma tecnológica, os sistemas de informação, os meios de armazenamento físico e as pessoas. Da mesma forma, atribuirá os responsáveis pelo tratamento dos incidentes de segurança da informação, que terão a responsabilidade de investigar e resolver os incidentes reportados, tomando as medidas necessárias para evitar a sua recorrência e escalando os incidentes de acordo com a sua criticidade. A Alta Direção ou quem por ela delegar são os únicos autorizados a reportar incidentes de segurança às autoridades; Da mesma forma, são os únicos canais de comunicação autorizados a fazer declarações oficiais a entidades externas.

Resposta a incidentes de segurança.

A área de Segurança da Informação deve designar pessoal qualificado para investigar adequadamente os incidentes de segurança relatados, identificando as causas, conduzindo uma investigação minuciosa, fornecendo soluções e por fim prevenindo sua recorrência.

Da mesma forma, determinar se o incidente afeta o Grupo Inngen e o seu impacto, tendo em conta o seguinte:

a) **BAJO:** Se o incidente for isolado e afetar apenas uma estação de trabalho interna ou associada. Este tipo de incidente também é definido como um problema do usuário final; é um evento que pode ser uma ameaça menor ou é resultado de atividade não autorizada, mas não compromete recursos críticos ou informações confidenciais.

b) **MEDIO:** Se o incidente afetar estações de um grupo de trabalho ou serviços operacionais internos, é um evento que pode ser uma ameaça futura, mas não é identificado como uma ameaça grave e/ou imediata.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	26 / 35

c) **ALTO:** É um evento muito crítico, no qual representa uma ameaça grave e afeta imediatamente um ou mais recursos críticos ou coloca em risco informações sensíveis ou confidenciais, o incidente envolve um ou mais usuários externos dos serviços.

Com base nesta classificação, leva-se em consideração o seguinte:

- Se o incidente for classificado como ALTO ou MÉDIO, formar a equipa que irá lidar com o incidente, incluindo os especialistas identificados na fase de deteção, tendo em conta o tipo de recursos informáticos afetados e o nível de especialização exigido.
- Monitora as ferramentas atuais de software e hardware e os registros de atividades do sistema para determinar as causas do incidente.
- Procede con las acciones documentadas de acuerdo con el tipo de incidente identificado, y al impacto definido.
- Se o impacto do incidente for BAIXO, as ações a seguir serão determinadas e o Formulário de Relatório de Incidente será preenchido.

Posteriormente, a área de Segurança da Informação deverá, com o apoio da área de Tecnologia e da Secretaria-Geral, criar bases de conhecimento para os incidentes de segurança apresentados com suas respectivas soluções, a fim de reduzir o tempo de resposta aos incidentes futuros, com base nessas bases de conhecimento..

15- Detecção de vulnerabilidade

A seguir serão detalhadas as etapas estipuladas para a detecção e gerenciamento de vulnerabilidades.

15.1 Execute testes de detecção de vulnerabilidades.

Área de execução: Gerencia de IT.

Inicia a execução de testes de penetração e inspeção de código em recursos de computação selecionados. A revisão é realizada a cada 45 dias no máximo (a cada 30 dias é o habitual).

- Extrai o relatório dos resultados do teste, gerado como saída do procedimento da atividade anterior.
- Continua com o tratamento e documentação das descobertas do monitoramento de segurança.

15.2 Categoria de vulnerabilidade

- Baixo
- Metade
- Grande Importância
- Críticas

Baja: Esta é uma vulnerabilidade fraca, pois é a que menos afeta o nosso sistema informático ou aplicação e, portanto, a que terá menos impacto sobre ele. É um tipo de vulnerabilidade que pode ser facilmente abordada e não teremos problemas em reduzir esse impacto.

Período de solução: 45 días (como máximo)

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	27 / 35

Media o Moderada: É também uma vulnerabilidade de rápida mitigação, embora neste caso tenha um impacto maior que o anterior. As consequências negativas desta fragilidade podem ser reduzidas de forma simples e para isso utilize ferramentas como auditorias ou configurações já estabelecidas anteriormente.

Período de solução: 30 dias (como máximo)

Grande importância: Vulnerabilidades mais perigosas, pois são exploradas para atacar rapidamente o sistema do computador ou a aplicação correspondente. O maior impacto negativo encontra-se na perda de confidencialidade dos dados ou recursos estabelecidos, assim como a integridade destes também é afetada.

Período de solução: 7 dias (como máximo)

Crítica: Esta é a pior vulnerabilidade que existe e a que pode trazer maiores consequências negativas ao nosso sistema. É um tipo de fraqueza que permite facilmente desenvolver-se e expandir-se por toda a rede e esta ação é realizada de forma autónoma, pelo que o utilizador não necessita de realizar nenhum movimento dentro do sistema para que o ataque ocorra.

Período de solução: 2 dias (como máximo)

Estado mitigação

Sim: A vulnerabilidade é 100% mitigada.

Parcialmente: A vulnerabilidade foi parcialmente resolvida, uma nova data deverá ser definida, considerando os prazos máximos por nível. *

No: A vulnerabilidade não foi resolvida, uma nova data deverá ser definida, considerando os prazos máximos por nível. *

* A gestão de TI deve liderar e garantir os meios/recursos necessários para cumprir os prazos estabelecidos nos diferentes níveis.

15.3 Identifique e valide vulnerabilidades analisando fontes de monitoramento

Área executora: Arquiteto de Segurança.

Identifica possíveis vulnerabilidades que poderiam ser exploradas para quebrar os controles de segurança do Grupo INNGEN, através da análise de fontes classificadas, considerando:

Resultados gerados pela ferramenta de monitoramento.

- a) Vulnerabilidades anteriores.
- b) Não conformidade com padrões de segurança
- c) Não conformidade com políticas de segurança

• Compila informações adicionais disponíveis, para confirmação ou esclarecimento da vulnerabilidade através:

- a) Conduzindo entrevistas.
- b) Observação visual do ambiente associado à vulnerabilidade.
- c) Solicitação de informações adicionais dos administradores de recursos de TI envolvidos.
- d) Verificação de documentos de aceitação de vulnerabilidade.

15.4 Classifique a vulnerabilidade.

Área executora: Gerencia de IT

• Classifica vulnerabilidades em categorias para análise levando em consideração:

- a) Resultados gerados pela ferramenta de monitoramento
- b) Relatórios anteriores
- c) Falhas de segurança.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	28 / 35

d) Relatórios de incidentes

15.5 Analise e documente a vulnerabilidade

Área executora: Gerencia de IT.

Se esta for uma vulnerabilidade comprovada, documente:

a) A vulnerabilidade identificada através de um relatório, incluindo a sua descrição, o impacto que pode causar, e acrescentando quaisquer comentários pertinentes que permitam a sua resolução, documentando os recursos informáticos e ativos de informação que podem ser diretamente afetados pela vulnerabilidade.

b) Recurso informático no qual foi identificada a vulnerabilidade.

c) Equipamentos ou informações residentes na área vulnerável.

d) Recomendações gerais para a sua solução. Mantém um registro das vulnerabilidades encontradas para controle e monitoramento.

15.6 Defina o plano de ação

Área executora: Gerencia

- Decide com base nos resultados da análise anterior ou noutros aspectos relevantes, se o risco é aceite ou se é aprovado o início da execução do plano de implementação.

- Se o risco for aceite:

a) Documenta a aceitação do risco por meio de ato, estabelecendo a justificativa da aceitação e seu prazo.

b) Notifique a área de segurança para modificar a linha de base da ferramenta de monitoramento.

- Define o plano de implementação e possíveis datas e custos.

- Preencha o Formulário de Controle de Mudanças de Infraestrutura.

15.7 Implementar mudanças ou relatar

Área executora: Gerencia

Executar o plano de ação estabelecido e certificar as mudanças.

- Caso não seja possível realizar nenhuma ação corretiva no curto prazo, documentar e informar a Gerência de Segurança da Informação, indicando os motivos.

15.8 Acompanhe o plano de ação

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	29 / 35

Área executora: Gerencia

Acompanha o desenvolvimento do plano proposto sobre as ações definidas e o tratamento da vulnerabilidade.

15.9 Ferramentas autorizadas para testes de vulnerabilidade

Burp Suite: Ele permite testes automatizados de exploração e verificação de vulnerabilidades.

Metasploit: Fornece informações sobre vulnerabilidades de segurança e ajuda no Pentesting e no desenvolvimento de assinaturas para sistemas de detecção de intrusões.

Nmap: Permite-nos obter informações sobre os computadores da nossa rede, é capaz de verificar quais hosts estão ativos, e até verificar se têm portas abertas, se estão filtrando as portas (têm firewall ativado), e até saber qual sistema operacional um determinado dispositivo está usando.

* A utilização de outras ferramentas deverá ser autorizada pelo Gerente Geral.

15.10 Política de “Pen Testing”

a. Definição: Os testes de penetração são avaliações de segurança controladas que tentam explorar vulnerabilidades em um ambiente para identificar pontos fracos antes que invasores mal-intencionados o façam.

b. Periodicidade:

- Testes anuais obrigatórios a partir do início da produção do serviço.
- Após qualquer alteração importante na infraestrutura ou no aplicativo.
- Quando for descoberta uma nova ameaça ou vulnerabilidade que possa afetar nossos sistemas.
- Testes trimestrais recomendados para sistemas críticos.

c. Critérios Gerais:

- Ambiente de teste: Os testes devem ser realizados em ambiente semelhante ao de produção, mas isolado para evitar interrupções.
- Contratação de Terceiros: Um acordo de confidencialidade e não danos deve ser assinado.
- Relatório: Após cada teste, deve ser gerado um relatório detalhado que inclui vulnerabilidades encontradas, dados de exposição, recomendações e um plano de ação.
- Correção: As vulnerabilidades críticas devem ser abordadas imediatamente, enquanto as menos impactantes devem ser programadas para correção com base no seu nível de risco.
- Notificação: Se forem encontradas vulnerabilidades críticas, a alta administração e as partes interessadas deverão ser informadas.
-

16- Treinamento

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	30 / 35

A seguir serão detalhados os passos estipulados para a sensibilização e formação dos funcionários em matéria de Segurança Informática.:

1- A proposta de treinamento é definida e elaborada

Área Ejecutora: Gabinete de Segurança da Informação.

Analisa métricas com base em eventos ocorridos, identificando vulnerabilidades detectadas que podem afetar políticas e procedimentos de segurança.

Rever os temas abordados nas sessões de formação anteriores, de forma a determinar as necessidades de melhoria que devem ser reforçadas na formação dos funcionários.

2- Define el plan de capacitación

Área Ejecutora: Gabinete de Segurança da Informação.

Estabelece o respetivo plano de formação para novos (indução) e antigos funcionários, determinando os temas a debater, os objetivos propostos, o público-alvo, os meios, a periodicidade, os responsáveis por cada tarefa, o calendário de atividades e a Metodologia a aplicar.

3- Executar e avaliar o plano de conscientização e treinamento

Área Ejecutora: Escritório de Segurança da Informação.

- Desenvolve as atividades de formação propostas no plano de formação.
- Avalie o nível de compreensão do tema, aplicando testes ao final dos mesmos.

4- Monitore o progresso do plano de treinamento

Área Ejecutora: Escritório de Segurança da Informação.

- Monitore as métricas do processo.
- Com base nos resultados, gerencia melhorias no esquema de conscientização.

17- Critérios para o uso de criptografia

Os serviços criptográficos devem ser usados de acordo com os seguintes padrões:

- Desenvolvimento de políticas
- Separação de uso de chaves
- Estabelecimento de períodos-chave de duração
- Estabelecimento de procedimentos de gestão chave
- Conformidade normativa

17.1 Desenvolvimento de políticas

A aprovação da Política de Segurança Criptográfica cabe ao Gestor de TI. Esta política de segurança criptográfica deve ser desenvolvida através das seguintes normas:

- Política de gerenciamento de chaves criptográficas
- Política de certificação.
- Política de autenticação.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	31 / 35

- Política de criptografia.

A Área Tecnológica GRUPO INNGEN é responsável por desenvolver a política de segurança criptográfica através dos instrumentos indicados.

17.2 Separação de uso de chave

Geralmente, uma chave será usada apenas para um uso específico — pelos seguintes motivos:

- A utilização da mesma chave para dois processos criptográficos diferentes pode enfraquecer a segurança de alguns destes processos.
- Limitar o uso de uma chave permite controlar os danos causados caso a chave seja comprometida.
- Alguns usos de chaves geram problemas colaterais, pois possuem durações ou períodos de conservação diferentes.

Esta diretriz não impede o uso da mesma chave para processos que oferecem mais de um serviço criptográfico.

É expressamente permitida a utilização da chave privada para solicitar a certificação digital da chave pública correspondente a uma entidade certificadora.

17.3 Principais períodos de duração

Geralmente, uma chave será usada por um período específico, ou período criptográfico, pelos seguintes motivos:

- A quantidade de informações protegidas por uma chave disponível pela análise criptográfica é limitada.
- A exposição é limitada no caso de um comprometimento importante.
- A utilização de um determinado algoritmo está limitada ao seu período estimado de utilização eficiente.
- O tempo disponível para tentar penetrar nos mecanismos de acesso lógico, físico e processual que protegem uma chave contra divulgação não autorizada é limitado.
- O período durante o qual a informação pode ser comprometida pela divulgação acidental de chaves ou material criptográfico a entidades não autorizadas é limitado.

Os seguintes períodos de criptografia recomendados são estabelecidos:

Tipo de Chave	Período de uso do emissor	Período de uso do receptor
Senha privada de assinatura	1-4 anos	
Senha pública de assinatura.	Varios anos (depende de la longitud da senha)	
Senha simétrica de autenticação	Hasta 2 anos	ate 3 anos adicionais
Senha privada de autenticação	1-4 anos	
Senha pública de autenticação	1-4 años	
Senha simétrica de criptografia de dados	até 2 anos	até 3 anos adicionais
Senha simétrica de envoltura de senhas	ate 2 anos	ate 3 anos adicionais
Senha (simétrica y asimétrica) de geração de números aleatórios	Até a geração de novas sementes	
Senha maestra simétrica	Hasta 1 año	
Senha privada de transporte de senha	Hasta 2 años	
Senha pública de transporte de senha	1-2 años	
Senha simétrica de negociación de senha	1-2 años	

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	32 / 35

Senha privada estática de negociação de senha	1-2 años
Senha pública estática de negociação de senha	1-2 años
Senha privada efímera de negociação de senha	Una transacción
Senha pública efímera de negociação de senha	Una transacción
Senha simétrica de autorización	Hasta 2 años
Senha privada de autorización	Hasta 2 años
Senha pública de autorización	Hasta 2 años

Para a decisão específica dos prazos de aplicação deverá ser realizada uma análise de risco, considerando os seguintes fatores:

- A força dos mecanismos criptográficos usados
- Proteção de mecanismos utilizando equipamentos criptográficos seguros
- O ambiente operacional (instalações de acesso controlado, equipamento de escritório ou terminal de acesso público)
- O volume de informações ou o número de transações que devem ser protegidas
- Classificação de segurança de dados
- A função de segurança envolvida (criptografia de dados, assinatura digital, produção de chaves, negociação ou proteção)
- O principal método de regeneração
- O método de atualização ou derivação de chaves
- O número de nós da rede que eventualmente compartilham uma chave
- O número de cópias de uma chave e distribuição das cópias
- Ameaças à segurança das chaves

As restrições derivadas das normas e políticas das entidades certificadoras externas também devem ser particularmente consideradas, uma vez que em muitos casos são as entidades certificadoras que definem os períodos criptográficos.

Neste sentido, é autorizada a aceitação de períodos criptográficos superiores aos recomendados, desde que sejam chaves garantidas em certificados reconhecidos e emitidos em conformidade com a legislação vigente.

17.4 Procedimentos de gerenciamento chave.

Serão estabelecidos os seguintes procedimentos em relação aos seguintes aspectos:

- Geração de chaves para diferentes sistemas e aplicações criptográficas.
- Geração e obtenção de certificados de chave pública.
- Distribuição de chaves aos usuários, incluindo ativação assim que tiverem sido recebidos. Armazenamento de chaves, incluindo como os usuários autorizados obtêm acesso às chaves.
- Alteração ou atualização de senhas, incluindo regras sobre quando devem ser alteradas ou atualizadas e qual o procedimento aplicável.
- Gerenciamento de chaves comprometidas.
- Revogação de chaves, incluindo a sua retirada ou desativação.
- Arquivamento de chaves, especialmente no caso de informações criptografadas que foram arquivadas.
- Destruição de chaves.
- Registro e auditoria de operações relacionadas ao gerenciamento de chaves.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	33 / 35

Os períodos de ativação e desativação das chaves devem ser definidos para reduzir o risco de comprometimento, de modo que as chaves só possam ser utilizadas por um período de tempo específico, com base nas circunstâncias e na análise de risco.

Devem ser definidos procedimentos para garantir a autenticidade das chaves públicas, através da utilização de autoridades certificadoras apropriadas.

17.5 Conformidade normativa

Os serviços criptográficos devem ser utilizados de acordo com a legislação em vigor em cada momento.

17.6 Funções e responsabilidades em relação à criptografia

O responsável pela implementação desta política é a Direção de TI do Grupo Inngen.

A área de TI é responsável pelo gerenciamento de chaves, incluindo a geração de chaves e a operação da infraestrutura criptográfica para segurança da informação.

17.7 Criação, modificação e atualização

É responsabilidade do Gerente Geral criar, modificar e atualizar as chaves criptográficas das aplicações do jantar.

Deverá cumprir os prazos estabelecidos em 17.3 e deixar comprovativos no sistema de Tickets (ver 8.6).

Revise o procedimento de atualização:

https://www.Inngenlabs.com/archivos/documentos/amex/rv/Evidencia_actualizacion_DINNERO_KEY.pdf

18- Procedimentos básicos de instalação: Rede, Notebook e Servidores.

18.1 Rede

- Firewall de perímetro: O objetivo do firewall de perímetro é impedir que sejam feitas conexões entre a rede corporativa e a Internet que estejam fora da política de segurança da empresa.

- Permissões de arquivos e pastas compartilhadas: É recomendável usar as opções da guia Segurança em vez da guia Permissões de compartilhamento.

- Protocolos de segurança: Recomenda-se utilizar as seguintes configurações:

- I. Protocolo TLS 1.2
- II. HTTP/2
- III. Cifrado simétrico
- IV. HTTPS

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	34 / 35

18.2 Notebook

- Atualizações do Sistema Operacional: A atualização do sistema operacional deve ser automática.
- Office: utilize o pacote Office 365 Professional.
- Cópia de arquivo: Todos os documentos devem ser replicados automaticamente para o OneDrive.
- Criptografia de disco: O disco deve ter criptografia BitLocker (padrão do Windows).
- Tipo de conta: a permissão de administrador não deve ser concedida.
- Login: A conta deve ser validada com o Active Directory.
- Firewall Local: Todas as portas de entrada devem ser bloqueadas.
- Instalação de antivírus: deverá ser utilizado o Norton 360.
- Instalação da rede Logmein Hamachi: É obrigatória para comunicação interna das equipes.
- Redirecionar conexões através do servidor proxy aprovado pela Administração.

18.3 Servidores

- Atualizações do Sistema Operacional: Desative a atualização automática, isso deve ser feito manualmente pelo Gestor de TI.
- Criptografia de disco: O disco deve ter criptografia BitLocker (padrão do Windows).
- Excluir usuário padrão: O usuário ADMINISTRADOR ou sua variante deve ser excluído.
- Definir senha segura: A seguinte combinação deve ser estabelecida:
 - I. Números
 - II. Letras
 - III. Maiúsculas e Minúsculas.
 - IV. caractere especial.
 - V. Mínimo 8 dígitos.
- Ativar Firewall: Deve permanecer automaticamente.
- Verificação de porta: Portas habilitadas:
 - I. 80 y 443 para http
 - II. 22 para Sftp

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PO.01		
		Data:	Rev.:	Pág.:
		20/01/2024	01	35 / 35

- Protocolos de segurança: Recomenda-se utilizar as seguintes configurações:
 - I. Protocolo TLS 1.2
 - II. HTTP/2
 - III. Cifrado simétrico
 - IV. HTTPS

- Instalação da rede Logmein Hamachi: É obrigatória para comunicação interna das equipes

Versión	Fecha actualización	Detalle	Autorizante
Versión 1.0	05-01-2015	Versión inicial	Ernet Marcelo
Versión 1.1	04-01-2016	Modificación y ajustes según necesidad. 2 - 4	Ernet Marcelo
Versión 1.2	04-01-2017	Ajustes de necesidad. 5.2 - 5.3	Ernet Marcelo
Versión 1.3	14-09-2017	Ajustes Extraordinario de necesidad 6.4 -6.5	Ernet Marcelo
Versión 1.4	04-01-2018	Modificación y ajustes según necesidad. 8 - 9	Ernet Marcelo
Versión 1.5	03-01-2019	Revisión de Política, sin modificaciones.	Ernet Marcelo
Versión 1.6	02-01-2020	Modificación y ajustes según necesidad. 13	Ernet Marcelo
Versión 1.7	04-01-2021	Verificación y modificación 14 – 15 - 17	Ernet Marcelo
Versión 1.8	27-01-2021	Verificación y modificación 8.6 - 10.3 -10.4 -18 -	Ernet Marcelo
Versión 1.9	22-03-2021	Verificación y modificación 13.6	Ernet Marcelo
Versión 2.0	05-05-2021	Verificación y modificación 10.4 -13.7	Ernet Marcelo
Versión 2.1	11-05-2021	Verificación y modificación 8.9	Ernet Marcelo
Versión 2.2	14-12-2021	Se agregó 17.7	Ernet Marcelo
Versión 2.3	01/05/2023	AXP revision	Ernet Marcelo
Versión 2.4	09/07/2023	AXP revisión	Ernet Marcelo
Versión 2.5	07/09/2023	Inclusión de política de “Pen Testing”	Ernet Marcelo
Version 2.6	28/09/2023	Inclusión de política de prevención de fuga de datos	Ernet Marcelo