Política Geral de Segurança da Informação

Gestamp Automoción, S.A.

27 Fevereiro 2023

ÍNDICE

1. Introdução

Nos termos do artigo 249.º-A da Lei das Sociedades Espanholas (a seguir «LSC») e do artigo 8.° do Regulamento do Conselho de Administração da Gestamp Automoción, S.A. (a «Sociedade»), compete ao Conselho de Administração aprovar as políticas gerais da sociedade.

Em virtude do exposto, o Conselho de Administração da Companhia, por meio da presente Política Geral de Segurança da Informação (a 'Política'), tem como objetivo ressaltar o compromisso da Companhia e de suas subsidiárias ('Gestamp' ou 'Grupo') com o cumprimento dos mais elevados padrões de segurança da informação.

2. Objetivo

O principal objetivo desta Política é estabelecer um marco regulatório aplicável ao Grupo, para a implementação de medidas de segurança que garantam a confidencialidade, integridade e disponibilidade de informações internas e de terceiros em poder da Gestamp.

Para este efeito, o âmbito da presente Política inclui a segurança física e digital, assegurando a implementação de medidas de segurança a nível organizacional, técnico e de pessoal, a fim de manter a continuidade dos negócios, prevenir fraudes, reduzir o risco de sofrer um ataque cibernético e proteger as informações de serem danificadas.

3. Âmbito de aplicação

Esta Política é aplicável ao Grupo Gestamp globalmente. Portanto, é aplicável a todas as subsidiárias do Grupo (não obstante os termos específicos estabelecidos na legislação aplicável a cada subsidiária), bem como à sua infraestrutura, redes, sistemas, equipamentos industriais, dispositivos e projetos em todas as áreas de negócio. Da mesma forma, o cumprimento desta Política é obrigatório para todos os colaboradores, pessoal externo e colaboradores da Gestamp que, para o desempenho de suas funções, necessitem manusear informações ou operar sistemas pertencentes à Gestamp.

Consequentemente, a presente Política deve ser disponibilizada a todos os colaboradores do Grupo, pessoas externas e colaboradores que se relacionem com o Grupo através de qualquer um dos seus processos.

4. Princípios

Os principais princípios de segurança da informação adotados pelo Grupo estão listados a seguir:

Segurança por design e por padrão. A Administração da Gestamp e cada uma das subsidiárias do Grupo comprometem-se a realizar, por projeto e por padrão, ações para estabelecer, operar, monitorar, manter, revisar e melhorar continuamente as medidas de segurança da informação, prestando especial atenção às questões de segurança cibernética em todo o Grupo. Nesse sentido, a área de Cibersegurança é responsável por definir metas e objetivos de segurança da informação, a fim de proteger a confidencialidade, integridade e disponibilidade dessas informações.

Legalidade, eficiência, corresponsabilidade, cooperação e coordenação. A Gestamp deve cumprir a presente Política, todos os requisitos legais, regulamentares, estatutários e contratuais aplicáveis, bem como os

requisitos estabelecidos por clientes, parceiros, órgãos governamentais, investidores e outras partes interessadas.

Responsabilidade proativa. As subsidiárias do Grupo, seus funcionários e seu pessoal externo e colaboradores devem ser capazes de demonstrar conformidade com a Estrutura Regulatória de Segurança. Para fazer isso, eles fornecerão todas as evidências necessárias.

Prevenção e melhoria contínua. A Gestamp estabeleceu uma estratégia preventiva para analisar os riscos aos quais a Companhia está exposta, identificando-os, implementando controles de mitigação e aplicando procedimentos regulatórios para fins de reavaliação. Ao longo desse processo de melhoria contínua, a Gestamp supervisionará a definição do nível de risco residual aceito (apetite ao risco), juntamente com os limites de tolerância da empresa.

Registro de incidentes. Todos os incidentes ou fraquezas que possam ou já tenham comprometido a confidencialidade, integridade e/ou disponibilidade das informações devem ser registrados e analisados para que as medidas corretivas/preventivas relevantes possam ser aplicadas.

Classificação da informação. A Gestamp classifica as informações para viabilizar processos de controle de acesso, custódia e monitoramento. Medidas preventivas e controles são estabelecidos de acordo com a classificação atribuída às informações. Quanto mais sensíveis forem as informações em questão, mais restritivos serão esses controles.

Limitações no tratamento de informações. O volume e o tipo de informação partilhada limitar-se-ão ao estritamente necessário para executar a tarefa para a qual a informação foi solicitada. Da mesma forma, o uso de qualquer informação fornecida será limitado aos fins para os quais foi autorizado.

Limitações de acesso à informação. O acesso à informação será limitado sempre que possível, a fim de garantir que só seja acessível a pessoas autorizadas. As informações de propriedade da Gestamp ou sob a guarda da Empresa só devem ser acessíveis a indivíduos autorizados, independentemente de pertencerem ou não ao Grupo.

Confidencialidade e integridade. As informações serão tratadas e divulgadas de forma a garantir a sua segurança, incluindo a proteção contra o acesso e utilização não autorizados/ilegais, perda, destruição ou danos acidentais dessas informações, através da aplicação das medidas técnicas ou organizativas adequadas.

Disponibilidade. A disponibilidade das informações deve ser garantida por meio da implementação de medidas adequadas de backup e continuidade de negócios.

Treinamento e conscientização. O pessoal com responsabilidades em matéria de segurança da informação deve estar equipado com os conhecimentos necessários para desempenhar as suas funções. Como tal, a Gestamp organizará atividades destinadas a reforçar o nível de sensibilização de todos os colaboradores relativamente à utilização da informação e ao cumprimento das medidas de segurança conexas.

5. Estrutura do Marco Regulatório de Segurança da Informação

O Marco Regulatório de Segurança é configurado por todas as políticas, regulamentos, procedimentos e diretrizes internas de segurança da informação aplicáveis ao Grupo. A estrutura hierárquica do Marco Regulatório de Segurança é a seguinte:

- Nível 1. Política Geral de Segurança da Informação. O presente documento constitui o principal componente do Marco Regulatório de Segurança. Estabelece propósitos de alto nível e o compromisso da Gestamp

  para gerenciar a segurança da informação, bem como os principais controles e princípios necessários para manter essas informações seguras. Os demais componentes do Marco Regulatório são

desenvolvidos e baseados nesta Política.

- Nível 2. Procedimentos e regulamentos de segurança. Um conjunto de documentos que dão suporte aos propósitos descritos na Política. Este nível descreve os requisitos de segurança para cada seção ou área incluída na Política com mais detalhes.
- Nível 3. Instruções de trabalho. Esses documentos detalham o conjunto de tarefas específicas que serão realizadas para dar suporte às operações diárias. Essas tarefas estão alinhadas com os requisitos de segurança estabelecidos nos procedimentos acima.

A presente Política, além dos requisitos estabelecidos nos procedimentos de segurança da informação e instruções de trabalho que compõem o Marco Regulatório de Segurança da Gestamp, deve ser cumprida por todos os colaboradores, além do pessoal externo e colaboradores do Grupo.

A Estrutura Regulatória de Segurança do Grupo é baseada nas melhores práticas e regulamentos de segurança da informação, como ISO/IEC 27001, NIST e Estruturas de Segurança Cibernética, e está sujeita a um processo anual de revisão e atualização.

6. Governança de Segurança da Informação

Estratégia e modelo operacional

A Gestamp formaliza o plano estratégico de segurança da informação da Companhia, que deve estar alinhado ao seu plano estratégico de negócios.

Os papéis e responsabilidades dos colaboradores do Grupo em relação à segurança da informação são definidos e atribuídos aos indivíduos apropriados. Dessa forma, a estratégia da Gestamp pode ser corretamente estruturada e desenvolvida, demonstrando a conformidade com o Marco Regulatório de Segurança. Isso garante uma segregação adequada de funções e evita potenciais conflitos de interesse. Para este efeito, as seguintes áreas podem ser delineadas:

- TI Corporativa da Gestamp. Esta é a área responsável por manusear, manter, suportar e melhorar as infraestruturas e sistemas corporativos e centralizados, além da conectividade entre esses componentes, aplicando sempre os mais altos padrões de qualidade e segurança. O alinhamento com o negócio e as necessidades de cada planta fabril e divisões é fundamental para garantir a entrega de serviços da mais alta qualidade.

- Área de Cibersegurança. Trata-se de uma subárea da TI Corporativa da Gestamp responsável pela definição de metas e objetivos de segurança da informação, com o objetivo de proteger a confidencialidade, integridade e disponibilidade das informações e supervisionar a execução da estratégia para gerenciar a segurança da informação. Isso será feito por meio da implementação de iniciativas que permitam que processos e infraestruturas sejam protegidos contra o crescente número de ameaças cibernéticas direcionadas ao setor, seguindo uma série de guias, regulamentos e padrões internacionais nos domínios Governança, Seguro, Vigilante e Resiliente.

- Comitê Tático de Cibersegurança. Esse Comitê é responsável por tomar decisões, gerenciar a estratégia de segurança cibernética e encaminhar informações para a Alta Administração. É composto pelo Chief Information Officer (CIO), pelo Gerente Corporativo de TI da Gestamp e pelos Gerentes das seguintes subáreas de TI Corporativa da Gestamp: o Gerente de Produção de TI, o Gerente de Cibersegurança e o Gerente de TI do GRC.

A Gestamp cumpre todos os requisitos legais, regulamentares e contratuais aplicáveis para os quais existe uma estrutura de controlo. Essa estrutura está associada ao Marco Regulatório de Segurança para verificar e monitorar os níveis de conformidade.

Uma estratégia de treinamento e conscientização em segurança da informação está em vigor para garantir que os funcionários da Gestamp desempenhem corretamente suas funções.

Cultura de segurança cibernética

A Gestamp promove uma cultura de segurança para enfrentar o risco cibernético em todos os níveis e envia anúncios e mensagens regulares sobre a estratégia de segurança cibernética e seus objetivos gerais.

Todos os funcionários do Grupo recebem treinamento em segurança cibernética regularmente durante todo o tempo em que estiverem na Empresa.

Gestão de riscos cibernéticos, indicadores e relatórios

A Gestamp possui uma metodologia de gestão de riscos cibernéticos que permite implementar planos de ação quando necessário. Ao mesmo tempo, realiza avaliações e análises de riscos cibernéticos para detectar os riscos cibernéticos aos quais o Grupo está exposto e gerenciá-los e reportá-los corretamente.

Com o objetivo de reduzir a subjetividade e melhorar a precisão das atividades de monitoramento e resposta a riscos cibernéticos, a Gestamp possui medidas quantitativas de risco cibernético (KPIs) que estão incluídas nos riscos operacionais.

7. Implantação de Controles de Segurança da Informação

7.1. Controle de acesso

A Gestamp deve regular o acesso de pessoal interno e externo aos sistemas de informação da empresa, bem como o tipo de informação processada ou armazenada, de acordo com as necessidades empresariais dos indivíduos. O acesso é concedido com base na estrita necessidade de conhecimento, ou seja, é concedido exclusivamente aos usuários que necessitam das informações ou de suas funções para a correta execução de suas tarefas, de acordo com sua função e perfil.

Os nomes de usuário devem ser exclusivos e intransferíveis. O princípio do privilégio mínimo deve ser inicialmente aplicado a todos os usuários, o que significa que eles recebem as permissões de acesso mínimas necessárias para executar suas funções.

As pessoas encarregadas do tratamento dos ativos de informação são responsáveis pela definição dos níveis de acesso e pela autorização de quaisquer permissões de acesso excecionais, em conformidade com as orientações da parte que concede a autorização ou dos gestores das informações em questão ou, se for caso disso, dos proprietários do processo ou da empresa.

7.2. Segurança no Desenvolvimento de Software

Os requisitos de segurança são aplicados em todo o ciclo de vida de desenvolvimento de software em vigor em
Gestamp, tanto em termos de software interno quanto de terceiros. Eles são aplicados durante a análise de requisitos e viabilidade, as fases em que esses requisitos são delineados e avaliados, bem como durante as fases de projeto, teste, implementação, aceitação e manutenção subsequente.

Para desenvolver corretamente o software, a Gestamp estabeleceu um plano de testes de segurança que inclui revisões seguras de código, mecanismos de proteção de dados, etc. Da mesma forma, o pentesting e a varredura de vulnerabilidades podem ser realizados em desenvolvimentos de software antes de serem

implantados.

A Gestamp garante que a segurança da informação seja parte integrante de seus processos e procedimentos de seleção, desenvolvimento e implementação de aplicativos, produtos e serviços.

A Gestamp informa os desenvolvedores de software sobre a presente Política e seus objetivos, bem como outros regulamentos internos que compõem o Marco Regulatório de Segurança.

7.3. Segurança do Sistema

A Gestamp estabeleceu formalmente responsabilidades e procedimentos documentados para garantir que os sistemas de informação sejam corretamente configurados, gerenciados, operados e monitorados.

Além disso, a Gestamp implementou medidas de proteção nos sistemas de informação para evitar ataques e vazamentos de dados. Estas medidas contribuem igualmente para garantir a segregação de funções na atribuição de responsabilidades, com o objectivo de evitar a utilização não autorizada dos sistemas de informação.

Para garantir a segurança dos sistemas, a Gestamp possui um processo de gerenciamento de patches que inclui as fases de base de software, disponibilidade, aplicabilidade, aquisição, validação e implantação dos ativos identificados.

A Gestamp executa a proteção do sistema para implementar corretamente a Estrutura Regulatória de Segurança, bem como fortalecer e definir claramente privilégios de usuário, grupos, funções e configurações de serviço.

7.4. Proteção contra malware

A Gestamp tem medidas em vigor para detectar, erradicar e proteger seus sistemas de informação contra diferentes tipos de malware conhecidos. As avaliações são realizadas pelo menos uma vez por ano, a fim de identificar e estudar quaisquer novas ameaças que tenham surgido. Dessa forma, a empresa pode confirmar quais novos sistemas podem ser expostos a essas ameaças e quais estão preparados para contê-las. Como resultado, todos os sistemas de informação da Gestamp possuem soluções atualizadas para proteção contra malware.

A Gestamp instalou o software EPP (End Point Protection) em todos os servidores e computadores que é atualizado automaticamente. Os utilizadores estão estritamente proibidos de desativar ou modificar mecanismos ou ferramentas EPP, a menos que estejam autorizados a fazê-lo e tenham recebido a autorização técnica necessária pela Área de Cibersegurança.

7.5. Segurança de Redes

A Gestamp gerencia e controla corretamente as redes com o objetivo de proteger a empresa contra ameaças e manter a segurança dos sistemas e aplicativos que utilizam a rede. Isso inclui o controle de acesso à rede, que é projetado para proteger todas as informações enviadas por meio desses elementos/ambientes.

As informações enviadas e recebidas por meio de redes de comunicação públicas e privadas são efetivamente protegidas por mecanismos de segurança que prezam pela confidencialidade, integridade e disponibilidade das informações. Os controles necessários são estabelecidos para evitar a falsificação do

remetente e a modificação ou perda de qualquer informação enviada em comunicações com sistemas de rede interna e quaisquer partes externas com as quais a Gestamp colabore.

Um conjunto de tecnologias e controles foram estabelecidos para conexão remota a redes Gestamp, dependendo de perfis de usuários individuais.

A rede Wi-Fi convidada é isolada das outras redes e é protegida por medidas de segurança que envolvem autenticação, monitoramento, criptografia, etc.

Todas as ligações às redes corporativas da Gestamp devem cumprir os requisitos técnicos estabelecidos pelo Grupo e quaisquer exceções devem ser previamente revistas e autorizadas pela Área de Cibersegurança.

7.6. Segurança de dispositivos do usuário final

A Gestamp estabeleceu diretrizes de uso e manuseio para dispositivos corporativos que aproveitam os serviços de informação pertencentes ao Grupo.

Os usuários não podem ser administradores locais de dispositivos corporativos aos quais eles têm acesso para fins de trabalho e não devem alterar o hardware ou as definições de configuração. É proibida a instalação de software que não tenha sido aprovado pela TI Corporativa da Gestamp.

7.7. Segurança de Recursos Humanos

As responsabilidades de segurança são tidas em conta durante todo o processo de recrutamento e preparação dos contratos. Os funcionários são então informados dessas responsabilidades assim que o contrato estiver em vigor, a fim de reduzir o risco de fraude ou o uso/adulteração/roubo inadequado de informações.

Nesse sentido, as políticas e regulamentações de segurança da informação da Gestamp se refletem nas obrigações contratuais dos funcionários. Os termos e condições discutem questões como confidencialidade, direitos legais e responsabilidades pelo cumprimento da Estrutura Regulatória de Segurança e pelo tratamento de informações de terceiros. As ações a serem tomadas em caso de descumprimento dos requisitos de segurança também são detalhadas.

Da mesma forma, a Gestamp informa a todos os colaboradores as responsabilidades de segurança da informação que são aplicáveis desde o momento em que são contratados até depois de terem saído oficialmente da empresa.

Todo o pessoal do Grupo participa de atividades de treinamento e conscientização em segurança da informação e é corretamente informado de suas funções e responsabilidades nessa área.

7.8. Segurança Física e Ambiental

As instalações do Grupo, incluindo escritórios e plantas de produção, nas quais ocorrem as operações de negócios, bem como as instalações internas ou de terceiros nas quais os sistemas de informação do Grupo estão localizados, são adequadamente protegidas por meio do uso de controles de acesso perimetral, CFTV e medidas de prevenção de acidentes, com o objetivo de prevenir a ocorrência de incidentes de segurança e/ou ambientais.

A Gestamp estabeleceu medidas de segurança para proteger os ativos físicos, juntamente com procedimentos para armazenar, manusear, transportar e destruir informações confidenciais em papel e

formato digital, a fim de mitigar o risco de acesso não autorizado e roubo.

7.9. Gestão da Informação

A Gestamp tem medidas de segurança em vigor para todas as fases do ciclo de vida das informações, incluindo criação, distribuição, manuseio, armazenamento e exclusão/destruição.

A Gestamp estabeleceu procedimentos e prazos para reter, armazenar e destruir informações, que são revisados e atualizados de acordo com a regulamentação aplicável.

A Gestamp classifica as informações corporativas para simplificar os processos de controle de acesso, custódia e monitoramento. Medidas preventivas e controles são estabelecidos de acordo com a classificação atribuída às informações. Quanto maior o nível de confidencialidade das informações em questão, mais restritivos serão esses controles.

7.10. Privacidade de Dados

Existem requisitos especiais de privacidade em vigor para sistemas e aplicativos que lidam com informações sensíveis ou pessoais, a fim de evitar que esses dados sejam roubados, divulgados ou acessados sem a devida autorização.

No que diz respeito à terceirização de processos da Gestamp que exigem que dados pessoais ou sensíveis sejam acessados ou tratados, contratos de processamento de dados e acordos de confidencialidade são estabelecidos com provedores de serviços externos, a fim de garantir que os dados permaneçam privados durante todo o seu ciclo de vida.

Para o efeito, a Gestamp tem em vigor uma Política de Proteção de Dados que detalha as garantias e princípios aplicáveis nesta área, juntamente com um conjunto de regulamentos, diretrizes e procedimentos adicionais concebidos para implementar exaustivamente os primeiros. A Gestamp adotou medidas técnicas e organizacionais para garantir a segurança dos dados pessoais e evitar a sua alteração, perda, tratamento ou acesso não autorizados, tendo em conta o estado da tecnologia, a natureza dos dados armazenados e os riscos a que estão expostos.

7.11. Segurança na nuvem

A Gestamp solicita todas as informações relacionadas aos controles e medidas de segurança aos provedores de serviços em Nuvem e verifica se esses controles estão alinhados com os padrões de segurança em Nuvem estipulados pela Gestamp.

Como resultado, a Gestamp garante que os provedores de serviços em nuvem tenham os mecanismos necessários para relatar incidentes de segurança que afetem a confidencialidade, integridade e disponibilidade das informações, de acordo com a legislação aplicável.

Além disso, o gerenciamento de incidentes e os planos de continuidade de negócios abrangem serviços terceirizados para provedores de serviços em nuvem. As auditorias necessárias também são realizadas para garantir a proteção do ambiente Cloud.

As informações armazenadas em ambientes de nuvem privada têm o mesmo nível de segurança que as informações que normalmente são armazenadas em infraestruturas pertencentes ao Grupo.

As informações armazenadas em ambientes de nuvem pública são previamente avaliadas pelo Comitê Tático de Cibersegurança, que define as medidas de segurança específicas a serem implementadas, levando em consideração uma série de técnicas de criptografia, anonimização, ofuscação e tokenização de informações.

7.12. Gestão de Riscos de Terceiros

A Gestamp dá ênfase especial à avaliação do nível de criticidade dos serviços que podem ser potencialmente terceirizados, o que ajuda a identificar aqueles que são relevantes do ponto de vista da segurança da informação devido à sua natureza, à sensibilidade dos dados a serem processados ou à sua dependência da continuidade dos negócios.

Os processos de recrutamento, os requisitos contratuais, o monitoramento do nível de serviço e as medidas de segurança implementadas por esses prestadores de serviços são priorizados pela Gestamp. Além disso, é obrigatória a apresentação de provas que demonstrem que o prestador de serviços em questão cumpre as normas fiscais e trabalhistas vigentes. Os controlos a que estes prestadores de serviços estão sujeitos são revistos anualmente.

A Gestamp tem processos formais em vigor para encerrar relações contratuais com prestadores de serviços, que incluem cláusulas contratuais específicas para garantir que as informações sejam mantidas privadas e devolvidas à empresa assim que o serviço for entregue.

7.13. Vigilante

Pentesting e varredura de vulnerabilidades

A Gestamp realiza a varredura de vulnerabilidades de acordo com o planejamento anual, com o objetivo de analisar a segurança de sistemas e aplicações e desenvolver planos de remediação. O escopo, a metodologia e a cobertura desses testes são ajustados de acordo com o nível de risco dos sistemas e funções, juntamente com a criticidade dos ativos em questão.

O Pentesting é realizado com uma variedade de prestadores de serviços, a fim de alterar as metodologias, garantindo que as melhorias sejam monitoradas para fazer antes e depois das comparações. Um processo de avaliação de risco é realizado durante a fase em que os pentests relevantes são selecionados.

Análise de segurança cibernética

A Gestamp tem processos em vigor para analisar o comportamento do usuário, a fim de detectar anomalias e padrões de ataque. Além disso, foram definidos processos para detectar atividades potencialmente nocivas e fraudulentas. Esses processos geram alertas que são enviados para a equipe de Resposta a Incidentes.

Além disso, as redes e sistemas da Gestamp são monitorados para detectar comportamentos anômalos.

Monitoramento de eventos de segurança

A Gestamp possui um serviço de gerenciamento de alertas e registro de eventos, correlação e monitoramento. Todas as atividades críticas são registradas e monitoradas por dispositivos de segurança.

A coleta e a correlação de registros são realizadas 24 horas por dia, 7 dias por semana, e são usadas para apoiar investigações, realizar análises forenses e fornecer evidências de conformidade regulatória.

Os registros são armazenados pelo sistema por pelo menos dois anos para que possam ser visualizados pela equipe autorizada pelo Grupo.

Nesse sentido, os registros só podem ser acessados pelos funcionários para fins relacionados ao trabalho. Além disso, os arquivos que armazenam esses logs são protegidos para evitar que modificações não autorizadas sejam feitas, e backups são criados para todos os logs.

Monitoramento de dispositivos e recursos de Tecnologia da Informação e Comunicação (TIC)

A Gestamp possui uma gama de dispositivos e recursos de TIC que são disponibilizados aos gestores e ao resto dos funcionários do Grupo. A empresa também possui as informações armazenadas nesses componentes.

Estes dispositivos e recursos de TIC e as informações que armazenam só podem ser utilizados por gestores e colaboradores da Gestamp para realizar tarefas relacionadas com o trabalho. Essas informações nunca devem ser usadas para assuntos pessoais/recreativos ou para realizar atividades ilegais.

A Gestamp tem a liberdade de processar, armazenar, monitorar, excluir ou destruir quaisquer dados armazenados permanente ou temporariamente em dispositivos e recursos de TIC sob a propriedade da Empresa, respeitando sempre a privacidade ou os direitos de propriedade intelectual/industrial, ou quaisquer outros interesses legítimos ou direitos estipulados na legislação aplicável.

7.14. Resiliente

Gestão de incidentes

A Gestamp definiu um processo de resposta a incidentes de segurança da informação para gerenciar corretamente todas as ameaças que possam se materializar dentro da Empresa. Esse processo inclui o monitoramento, a classificação e a remediação de incidentes.

Todos os incidentes que possam ou já tenham comprometido a confidencialidade, integridade e/ou disponibilidade das informações são registrados e analisados para que as medidas corretivas/preventivas relevantes possam ser aplicadas de acordo com o Procedimento de Gerenciamento de Incidentes da Gestamp.

Todos os colaboradores internos e externos são responsáveis por reportar aos gestores de segurança da Empresa quaisquer atividades suspeitas, incidentes ou crimes que possam comprometer a segurança dos ativos de informação pertencentes ao Grupo.

Além disso, foi estabelecido um plano anual de simulação de incidentes com o objetivo de treinar e conscientizar os colaboradores do Grupo.

Gerenciamento de continuidade de negócios

A Gestamp definiu um plano de continuidade de negócios para garantir que os serviços essenciais possam continuar a ser prestados e que quaisquer impactos nos negócios sejam adequadamente gerenciados em caso de crise. Isto é conseguido através da disponibilização de um quadro de referência que define como proceder nestas circunstâncias.

Este plano não discute apenas os planos de contingência do sistema de informação, mas também as dependências físicas, os indivíduos que suportam as operações de negócios e os recursos que podem ser necessários para que essas operações do Grupo sejam mantidas em funcionamento e que os serviços possam ser fornecidos aos clientes.

O plano de contingência é desenvolvido e implementado para garantir que os processos críticos de negócios possam ser restabelecidos o mais rápido possível. Inclui controles projetados para identificar e reduzir riscos, limitar as consequências de incidentes e determinar o tempo de resposta de operações essenciais. A formação atribuída à equipa de Gestão de Crises, exercícios de simulação e revisões regulares dos procedimentos de resposta definidos são fundamentais para este plano.

Este plano é publicado e revisado anualmente ou em resposta a mudanças importantes, como a inclusão de novos ativos imobiliários, tecnológicos ou organizacionais.

Todas as informações sensíveis, confidenciais e pessoais são armazenadas em backups, que são gerenciados de acordo com as medidas de segurança definidas pela Gestamp.

8. Conformidade

A Gestamp deve assegurar o cumprimento desta Política anualmente.

A Gerência da Gestamp comprometer-se-á a incentivar e apoiar a implementação de medidas técnicas, organizacionais e de controlo que garantam a autenticidade, confidencialidade, integridade, disponibilidade e auditabilidade das informações.

A gestão desta Política corresponde à Área de Cibersegurança, que deve, portanto, interpretar quaisquer dúvidas que possam surgir em sua aplicação, bem como proceder à revisão da mesma quando necessário ou necessário, para propor a atualização de seu conteúdo. A Gerência de Auditoria Interna do Grupo tem o direito de realizar quantas análises e verificações julgar apropriadas para confirmar que esta Política está sendo corretamente implementada.

O Comitê de Auditoria supervisionará anualmente o cumprimento desta Política e reportará quaisquer conclusões ao Conselho de Administração.

Ações disciplinares podem ser tomadas em caso de violação da Política. Todos os colaboradores internos e externos são responsáveis por reportar à Área de Cibersegurança qualquer evento ou situação que possa resultar no não cumprimento desta Política.

9. Exceções

A Área de Cibersegurança deve ser informada de quaisquer exceções a esta Política para que possam ser aprovadas antes da implementação e devidamente registradas.

10. Referências

A presente Política está em conformidade com as seguintes normas e regulamentos internacionais de segurança da informação:

- ISO/IEC 27001 'Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos'.
- ISO/IEC 27002 'Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação'.
- Regulamento Geral de Proteção de Dados (RGPD).
- Estrutura de Cibersegurança.

11. Aprovação e revisão

Esta Política foi aprovada pelo Conselho de Administração da Companhia e quaisquer modificações feitas nesta Política deverão ser aprovadas por esta Política, mediante proposta do Comitê de Auditoria.

Esta Política será revisada anualmente pelo Comitê Tático de Cibersegurança em conjunto com a Área de Cibersegurança.

Versão	Parte emissora	Supervisor	Partido de aprovação	Entidade	Data de aprovação
1.0	TI Corporativa	Comitê de Auditoria	Diretoria da Diretores	GECARIMBO AUTOMOCIÓN, Sa	27 Fevereiro 2023

Version	Description	Edited by	Approved by	Date of approval
1.0	Revision without update	GRC IT Office	Cybersecurity Responsible	18/07/2024
1.1	Revision without update	GRC IT Office	Cybersecurity Responsible	22/05/2025