Política de Segurança

Política de Segurança

Índice do conteúdo

1. Introdução

Este documento define a Política de Segurança da Informação da MHP SERVICIOS DE CONTROL S.L (MHP), como o conjunto de princípios básicos e linhas de conduta em que a Organização está comprometida, no âmbito das Normas ISO 27001 e do Esquema Nacional de Segurança (ENS).

A informação é um ativo crítico, essencial e de grande valor para o desenvolvimento da atividade da empresa. Este ativo deve ser adequadamente protegido, através das medidas de segurança necessárias, face às ameaças que o possam afetar, independentemente dos formatos, suportes, meios de transmissão, sistemas, ou pessoas que intervêm no seu conhecimento, processamento ou tratamento.

A Segurança da Informação é a proteção deste ativo, a fim de assegurar a qualidade da informação e a continuidade do negócio, minimizar o risco e permitir maximizar o retorno dos investimentos e as oportunidades do negócio.

A segurança da informação é um processo que requer recursos técnicos e humanos e uma gestão e definição adequadas dos procedimentos e no qual é essencial a máxima colaboração e envolvimento de todo o pessoal da empresa.

A direção da empresa, consciente do valor da informação, está profundamente comprometida com a política descrita no presente documento.

2. Definições

- **Sistema de Informação:** Conjunto organizado de recursos para que informação possa ser recolhida, armazenada, processada ou tratada, mantida, utilizada, partilhada, distribuída, disponibilizada, apresentada ou transmitida.

- **Risco:** Estimativa do grau de exposição a uma ameaça que se materializa em um ou mais ativos causando danos ou prejuízos à organização.

- **Gestão de riscos:** Atividades coordenadas para dirigir e controlar uma organização no que diz respeito aos riscos.

- **Sistema de Gestão de Segurança da Informação (SGSI):** Sistema de gestão que, baseado no estudo dos riscos, é estabelecido para criar, implementar, operar, supervisionar, rever, manter e melhorar a segurança da informação. O sistema de gestão inclui a estrutura organizativa, as políticas, as atividades de planeamento, as responsabilidades, as práticas, os procedimentos, os processos e os recursos.

- **Disponibilidade:** Há necessidade de assegurar que os recursos do sistema estejam disponíveis quando necessário, especialmente a informação crítica.

- **Integridade:** A informação do sistema deve estar disponível conforme armazenada por um agente autorizado.

- **Confidencialidade:** A informação deve estar disponível apenas para agentes autorizados, especialmente o seu proprietário.

- **Autenticidade**: (relacionada com o ENS). A identidade ou a origem da informação deve ser assegurada.

- **Rastreabilidade**: (relacionado com o ENS). SDeve ser assegurado para certos dados quem fez o quê e em que momento.

MHP Servicios de Control, S.L. B35664879 inscrita en el Registro Mercantil de Las Palmas, tomo 1559, folio 189, sección 8, hoja GC-26515

3. Finalidade

A finalidade desta Política de Segurança da Informação é proteger os ativos de informação da MHP, assegurando a disponibilidade, integridade, confidencialidade, autenticidade e rastreabilidade da informação e das instalações, sistemas e recursos que a processam, gerem, transmitem e armazenam, sempre de acordo com os requisitos de negócio e a legislação vigente.

4. Alcance

O Sistema de Gestão de Segurança especificado neste Manual de forma consistente com a norma internacional UNE-ISO/IEC 27001:2017 e o Esquema Nacional de Segurança tem o seguinte alcance, que em qualquer caso se reflete também na análise do Contexto Organizacional SGSI 02:

"Os sistemas de informação que suportam os seguintes serviços geridos pela entidade MHP Servicios de Control, S.L., com sede social na Avenida Alcalde Ramírez Bethencourt, n.º 12, Centro de Oficinas Fuentemar, C.P 35004, Las Palmas de Gran Canaria: sistemas de controlo horário e de presença através de terminais próprios ou outros dispositivos, a plataforma de gestão de registo horário e presença, consultoria e atendimento ao cliente"

A presente Política de Segurança da Informação aplica-se a todas as pessoas, sistemas e meios que acedam, tratem, processem, armazenem, transmitam ou utilizem a informação conhecida, gerida ou propriedade da empresa para os processos descritos.

O pessoal sujeito a esta política inclui todas as pessoas com acesso às informações descritas, independentemente de as informações serem ou não automatizadas e de o indivíduo ser ou não funcionário da empresa. Por conseguinte, também se aplica a empreiteiros, clientes ou qualquer outro terceiro que tenha acesso às informações ou sistemas da empresa.

Para assegurar que o processo de segurança implementado será continuamente atualizado e melhorado, é implementado e documentado um Sistema de Gestão de Segurança da Informação. Desta forma, o conteúdo da Política de Segurança da Informação é desenvolvido em normas e procedimentos de segurança complementares.

5. Objetivos e fundamentos da política

A informação deve ser protegida durante todo o seu ciclo de vida, desde a sua criação ou receção, durante o seu processamento, comunicação, transporte, armazenamento, disseminação e mesmo a sua eventual eliminação ou destruição. Por conseguinte, são estabelecidos os princípios mínimos seguintes:

- **Princípio da confidencialidade**: os sistemas de informação devem ser acessíveis apenas aos utilizadores, organismos e entidades ou processos expressamente autorizados para o efeito, no que respeita às obrigações de sigilo e confidencialidade profissional.

- **Princípio da integridade e qualidade**: a integridade e qualidade da informação deve ser garantida, bem como os processos para o seu tratamento, estabelecendo mecanismos para assegurar que os processos de criação, tratamento, armazenamento e distribuição da informação contribuem para preservar a sua exatidão e correção.

- **Princípio da disponibilidade e continuidade**: será garantido um nível de disponibilidade nos sistemas de informação e serão fornecidos os planos e medidas necessários para assegurar a continuidade dos serviços e a recuperação no caso de possíveis contingências graves.

- **Princípio da gestão dos riscos**: um processo contínuo de análise e tratamento dos riscos deve ser articulado como um mecanismo básico no qual se deve basear a gestão da segurança dos sistemas de informação.

- **Princípio da proporcionalidade nos custos**: a implementação de medidas que atenuem os riscos de segurança dos sistemas de informação deve ser feita sob uma abordagem de proporcionalidade nos custos económicos e operacionais, sem prejuízo de assegurar a disponibilidade dos recursos necessários para o sistema de gestão da segurança da informação.

- **Princípio da sensibilização e formação**: serão articuladas iniciativas para permitir aos utilizadores conhecer os seus deveres e obrigações relativamente ao tratamento seguro da informação. Do mesmo modo, será promovida a formação específica em termos de segurança das TIC para todas aquelas pessoas que gerem e administram sistemas de informação e telecomunicações.

- **Princípio da prevenção**: serão desenvolvidos planos e linhas de trabalho específicos para prevenir a fraude, o incumprimento ou incidentes relacionados com a segurança das TIC.

- **Princípio da deteção e resposta**: os serviços devem monitorizar continuamente a operação para detetar anomalias nos níveis de prestação dos serviços e agir em consequência, respondendo eficazmente, através dos mecanismos estabelecidos para o efeito, aos incidentes de segurança.

- **Princípio da melhoria contínua**: o grau de cumprimento dos objetivos de melhoria da segurança anualmente planeados e o grau de eficácia dos controlos de segurança das TIC implementados serão revistos, a fim de os adaptar à constante evolução dos riscos e do ambiente tecnológico da Administração Pública.

- **Princípio da segurança das TIC no ciclo de vida dos sistemas de informação**: as especificações de segurança serão incluídas em todas as fases do ciclo de vida dos serviços e sistemas, acompanhadas dos correspondentes procedimentos de controlo.

- **Princípio da função diferenciada**: a responsabilidade pela segurança dos sistemas de informação será diferenciada da responsabilidade pela prestação dos serviços.

A Política de Segurança da Informação é aprovada pela Direção da empresa e do seu conteúdo e a das regras e procedimentos que a desenvolvem é de cumprimento obrigatório:

- Todos os utilizadores com acesso à informação tratada, gerida ou propriedade da empresa têm a obrigação e o dever de a salvaguardar e proteger.

- A Política e as Normas de Segurança da Informação serão adaptadas à evolução dos sistemas e da tecnologia e às mudanças organizativas, e serão alinhadas com a legislação em vigor e com os padrões e as melhores práticas da norma ISO/IEC 27001:2014 e do Esquema Nacional de Segurança.

- As medidas de segurança e os controlos físicos, administrativos e técnicos aplicáveis serão detalhados no Documento de Aplicabilidade e a empresa terá de estabelecer um planeamento para a sua implementação e gestão.

- As medidas de segurança e os controlos estabelecidos serão proporcionais à criticidade da informação a proteger e à sua classificação.

- Os utilizadores que não cumpram a Política de Segurança da Informação ou as regras e procedimentos complementares podem ser sancionados de acordo com as disposições dos contratos que regem a sua relação com a empresa e com a legislação em vigor e aplicável.

6. Objetivos e fundamentos da política

Esta política de segurança será desenvolvida mediante a aplicação dos seguintes critérios:

6.1 Organização e implementação do processo de segurança.

A segurança da informação compromete todos os membros da organização. A MHP identifica os responsáveis e estabelece as suas responsabilidades na secção "Papéis, Responsabilidades e Deveres" deste documento. A política de segurança e os regulamentos serão conhecidos por todos os membros da organização.

6.2 Análise e gestão dos riscos.

Conhecer os riscos e elaborar uma estratégia para os gerir adequadamente é fundamental para a empresa, uma vez que só se o estado da segurança for conhecido é que as decisões adequadas poderão ser tomadas para mitigar os riscos aos quais está exposto.

A MHP utiliza a metodologia **Magerit** para analisar os riscos, realizando uma análise detalhada dos riscos que atingem os ativos recolhidos num inventário de ativos, que está documentado num documento de Análise de Riscos.

A entidade determina os níveis de risco a partir dos quais toma medidas de tratamento sobre os mesmos. Um Risco é considerado aceitável quando se estima que a implementação de mais controlos de segurança consumirá mais recursos do que o possível impacto associado.

Uma vez realizado o processo de avaliação de riscos, a direção da empresa é a responsável pela aprovação dos riscos residuais e dos planos de tratamento de riscos.

6.3 Gestão de pessoal.

Todo o pessoal da MHP relacionado com informação e sistemas é formado e informado dos seus deveres e obrigações de segurança, essencialmente através dos procedimentos de segurança adequados e através de regulamentos sobre a utilização de ativos. As suas ações são supervisionadas de acordo com os papéis estabelecidos para verificar que os procedimentos definidos são seguidos.

Os acessos dos utilizadores são únicos e os seus direitos e as atividades que têm a ver com a Segurança da informação são verificados periodicamente para corrigir ou exigir responsabilidades no seu caso.

6.4 Profissionalismo, Sensibilização e Formação.

A segurança dos sistemas é gerida e revista por pessoal qualificado da MHP e pessoal externo especializado, que recebe e atualiza a formação necessária para garantir a segurança da informação.

A presente Política de Segurança da Informação deve ser conhecida por todos os utilizadores internos e externos e pelas empresas que acedem, gerem ou tratam os dados da empresa.

O conjunto de Políticas, normas e procedimentos complementares a esta Política de Segurança da Informação deverá também ser adequadamente comunicado e dado a conhecer às pessoas, empresas e instituições afetadas ou envolvidas em cada caso.

Os programas de comunicação, sensibilização e formação serão definidos periodicamente e será fornecido aos utilizadores um exemplar dos regulamentos correspondentes.

6.5 Autorização e controlo dos acessos.

O acesso aos sistemas de informação é controlado, monitorizado e limitado aos utilizadores, processos, dispositivos e sistemas de informação com as funcionalidades mínimas permitidas e/ou autorizadas.

6.6 Proteção física das instalações.

Os sistemas da MHP estão localizados em áreas devidamente protegidas, equipadas com medidas de segurança física, redundância, continuidade e ambiente, e com um procedimento de controlo de acesso.

6.7 Segurança por defeito.

Na MHP, os sistemas são concebidos e configurados sempre tendo em vista a Segurança por Defeito. O sistema fornece a funcionalidade mínima necessária e a MHP assegura que só são acessíveis por pessoas, e a partir de locais ou equipamentos autorizados. Isto é particularmente importante em sistemas operacionais, onde a MHP remove, desativa (ou aconselha a desativar ou remover, conforme o caso) funções que não devam ser utilizadas.

Todos os projetos relacionados ou que afetem os sistemas de informação devem incluir, no seu processo de análise, uma avaliação dos requisitos de segurança e definir um modelo de segurança acordado com o responsável pela segurança da informação.

No desenho, desenvolvimento, instalação e gestão de sistemas de informação e nos projetos devem ser tidos em conta e aplicados conceitos de segurança desde o desenho, codificação segura e os controlos e medidas de segurança adequados de acordo com o documento de aplicabilidade aprovado pela empresa.

6.8 Contratação e aquisições.

Todas as contratações e aquisições que envolvam ou exijam acesso ou tratamento da informação classificada como não pública serão feitas ao abrigo de um contrato que inclua cláusulas destinadas a assegurar a salvaguarda da confidencialidade, integridade e disponibilidade da informação.

Nos casos em que os serviços contratados implicam o acesso ou tratamento pelo fornecedor de dados pessoais, o contrato deve incluir as cláusulas necessárias para o cumprimento da LOPDGDD e os seus desenvolvimentos.

As empresas e pessoas que, para efeitos de contratação de serviços ou aquisições de qualquer tipo, acedam à informação confidencial ou informação de uso interno, devem ter conhecimento da Política de Segurança da Informação e das regras e procedimentos complementares aplicáveis ao objeto do contrato.

As empresas e pessoas externas que acedam à informação da empresa devem considerar tal informação, por defeito, como confidencial. A única informação que pode ser considerada como não confidencial é a obtida através dos meios de comunicação públicos.

6.9 Integridade e atualização do sistema.

Na MHP, os sistemas são avaliados periodicamente a fim de conhecer o seu estado de segurança a todo o momento, tendo em conta as especificações dos fabricantes, as vulnerabilidades e as atualizações adequadas, e assim gerir a integridade dos mesmos.

Todos os elementos dos sistemas necessitam de autorização prévia para a sua instalação.

6.10 Proteção da informação armazenada e em trânsito.

A informação é classificada de acordo com a sensibilidade exigida no seu tratamento e de acordo com os níveis de segurança e proteção exigidos.

A MHP presta especial atenção à informação armazenada ou em trânsito através de ambientes inseguros. Isto inclui informação armazenada ou tratada em computadores portáteis, tablets, smartphones, dispositivos periféricos, suportes de informação, bem como comunicações em redes abertas ou fracamente encriptadas, onde são aplicadas medidas de segurança para assegurar que a informação é tratada de acordo com a sua classificação.

6.11 Prevenção face a outros sistemas de informação interligados.

A MHP protege o perímetro de acesso ao seu sistema, em particular nas ligações através da Internet, analisando sempre os riscos derivados da interligação com outros sistemas, e estabelecendo as medidas que garantem o nível de segurança necessário.

6.12 Registo de atividade.

A MHP regista as atividades dos seus utilizadores a fim de monitorizar, analisar, investigar e documentar atividades impróprias ou não autorizadas, permitindo a identificação da pessoa que atua em qualquer momento. Tudo isto é feito com total garantia do direito à honra, à privacidade pessoal e familiar e à imagem das pessoas afetadas, e em conformidade com os regulamentos de proteção de dados pessoais e outras disposições aplicáveis.

6.13 Incidentes de segurança.

Qualquer compromisso com a confidencialidade, integridade, disponibilidade, autenticidade ou rastreabilidade da informação da empresa é considerado um incidente de segurança.

A MHP tem um sistema de deteção e reação face a incidentes de segurança, que são classificados e geridos até serem resolvidos através da recolha de provas para que possam ser relatados e aprendidos com eles para uma melhoria contínua.

Em particular, a empresa possui um sistema de deteção e reação face a códigos nocivos, bem como um sistema de prevenção e deteção de intrusões, realizando auditorias técnicas para assegurar as medidas de proteção pertinentes.

Os utilizadores têm canais estabelecidos para reportar imediatamente qualquer incidente ou anomalia detetada.

6.14 Continuidade da atividade.

A MHP faz backups para assegurar a recuperação da informação, e estabelece mecanismos apropriados para assegurar a continuidade das operações em caso de perda dos recursos de trabalho normais.

6.15 Melhoria contínua do processo de segurança.

O sistema de gestão de segurança implementado é continuamente atualizado e melhorado, tal como estabelecido pelas certificações ISO 27001 e do Esquema Nacional de Segurança.

7. Requerimentos Legais

- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais (RGPD).

- Lei Orgânica 3/2018, de 5 de Dezembro, sobre Proteção de Dados e Garantia dos Direitos Digitais (LOPDGDD).

- Real Decreto Legislativo 1/1996, de 12 de Abril de 1996, Lei da Propriedade Intelectual.

- Lei 34/2002 de 11 de Julho, sobre serviços da sociedade da informação e comércio eletrónico.

- Real Decreto 3/2010, de 8 de Janeiro, que regulamenta o Esquema Nacional de Segurança.

- Real Decreto 951/2015, de 23 de Outubro que altera o Real Decreto 3/2010 de 8 de Janeiro que regulamenta o Esquema Nacional de Segurança.

8. Papéis, Responsabilidades e Deveres

A direção atribui, renova e comunica as responsabilidades, autoridades e papéis relativos à segurança da informação, determinando em cada caso as razões, o prazo de validade, e gerindo os conflitos que possam surgir. Também assegurará que os utilizadores estejam cientes, assumam e exerçam as responsabilidades, autoridades e papéis atribuídos.

8.1 Utilizadores

Qualquer pessoa ou sistema que aceda à informação tratada, gerida ou propriedade da empresa será considerada um utilizador. Os utilizadores são responsáveis pela sua conduta ao acederem à informação ou ao utilizarem os sistemas informáticos da empresa. O utilizador é responsável por todas as ações realizadas utilizando os seus identificadores pessoais ou credenciais.

Os utilizadores têm a obrigação de o fazer:

- Cumprir a Política de Segurança da Informação e as regras, procedimentos e instruções complementares.

- Proteger e salvaguardar a informação da empresa, evitando a divulgação, emissão para o exterior, modificação, apagamento ou destruição acidental ou não autorizada ou a utilização indevida, independentemente do suporte ou meio pelo qual foi acedida ou conhecida.

- Conhecer e aplicar a Política de Segurança da Informação, as Normas de Uso dos Sistemas de Informação e o resto das políticas, regras, procedimentos e medidas de segurança aplicáveis.

8.2 Responsável pela Informação (Esquema Nacional de Segurança)

O Responsável pela Informação é o último responsável por qualquer erro ou negligência que envolva um incidente de confidencialidade ou integridade (em termos de proteção de dados) e disponibilidade (em termos de segurança da informação).

O Responsável pela Informação tem as seguintes responsabilidades:

- Velar pela utilização adequada da informação e, por conseguinte, pela sua proteção.
- Estabelecer os requisitos de informação em termos de segurança.
- Determinar os níveis de segurança da informação tratada, avaliando as consequências de um impacto negativo.

Dado o acima exposto, o papel de Responsável pela Informação na MHP é assumido pelo Gerente da Organização.

8.3 Responsável de Serviço (Esquema Nacional de Segurança)

O proprietário dos ativos do Serviço, entendendo como tal a pessoa encarregada do referido serviço, terá as seguintes responsabilidades gerais:

- O proprietário dos ativos do Serviço, entendendo como tal a pessoa encarregada do referido serviço, terá as seguintes responsabilidades gerais.
- Determinar os níveis de segurança do serviço, em acordo com o Responsável pela Segurança e o Responsável do Sistema.
- Manter a segurança da informação manipulada e dos serviços prestados pelos sistemas de informação no seu âmbito de responsabilidade.

A figura do Responsável de Serviço da MHP é assumida pelo Gerente da Organização.

•

8.4 Direção

A direção da MHP está profundamente comprometida com a política descrita neste documento e está consciente do valor da informação e do grave impacto económico e de imagem que um incidente de segurança pode causar.

No contexto do Esquema Nacional de Segurança, a Direção assume as responsabilidades descritas para o Responsável pela Informação e para o Responsável do Serviço.

A Direção é, portanto, a proprietária dos ativos de informação próprios da MHP, e também a proprietária dos riscos.

A Direção também assume as seguintes responsabilidades:

- Demonstrar liderança e compromisso com o sistema de gestão da segurança da informação.
- Assegurar que a política e os objetivos de segurança da informação são estabelecidos e são compatíveis com a direção estratégica da organização.
- Aprovar e comunicar a Política de Segurança da Informação, as Normas de Uso dos Sistemas de Informação e a importância do seu cumprimento a todos os utilizadores, internos ou externos, aos clientes e fornecedores.
- Reunir-se **trimestralmente**, e quando qualquer evento ou pedido extraordinário o exigir, com os Responsáveis pela Segurança e dos Sistemas, para ser informado sobre o SGSI e para atualizar a estratégia sobre Segurança da Informação.
- Promover uma cultura empresarial de segurança da informação, promovendo a Sensibilização e aprovando planos de formação.

- Apoiar a melhoria contínua dos processos e projetos de segurança da informação.

- Assegurar que estão disponíveis os recursos necessários para o cumprimento da política de segurança da informação, das normas de uso dos sistemas e do funcionamento do sistema de gestão da segurança da informação.

- Definir a abordagem da análise e da gestão dos riscos de segurança da informação e os critérios para assumir os riscos e assegurar a avaliação desses riscos pelo menos anualmente, exercendo para esse efeito o papel de proprietário dos riscos.

- Assegurar a realização de auditorias internas de segurança da informação e a revisão dos seus resultados para identificar oportunidades de melhoria.

- Definir e controlar o orçamento para a segurança da informação.

- Aprovar a documentação até ao seu segundo nível de regras e procedimentos.

- Determinar as medidas, sejam elas disciplinares ou quaisquer outras, que pudessem ser aplicadas aos responsáveis por violações de segurança.

8.5 Responsável pela Segurança

A pessoa com o cargo de Responsável pela Segurança da Informação assumirá as seguintes funções:

- Promover a segurança da informação manipulada e dos serviços eletrónicos fornecidos pelos sistemas de informação, com a responsabilidade e autoridade de assegurar que o Sistema de Gestão de Segurança da Informação cumpre os requisitos do Esquema Nacional de Segurança e da Norma UNE-ISO/IEC 27001.

- Supervisionar o cumprimento desta Política, das suas normas, dos procedimentos derivados e da configuração de segurança dos sistemas.

- Estabelecer as medidas de segurança, adequadas e eficazes para satisfazer os requisitos de segurança estabelecidos pela Direção, seguindo sempre as exigências do Anexo II do ENS, declarando a aplicabilidade de tais medidas.

- Promover as atividades de sensibilização e formação em matéria de segurança no seu âmbito de responsabilidade.

- Coordenar e acompanhar a implementação dos projetos de adaptação às normas especificadas (ISO 27001 e ENS), em colaboração com o Responsável dos Sistemas.

- Realizar, com a colaboração do Responsável do Sistema, as análises de risco necessárias, selecionar as salvaguardas a serem implementadas e rever o processo de gestão de risco. Do mesmo modo, em conjunto com o Responsável do Sistema, aceitar os riscos residuais calculados na análise de riscos.

- Promover auditorias periódicas para verificar o cumprimento das obrigações de segurança da informação e analisar os relatórios de auditoria, preparando as conclusões a apresentar ao Responsável de Sistemas para as devidas ações corretivas.

- Coordenar o processo de Gestão da Segurança, em colaboração com o Responsável dos Sistemas.

- Assinar a Declaração de Aplicabilidade, que inclui a lista de medidas de segurança selecionadas para um sistema.

- Elaborar relatórios periódicos de segurança que incluam os incidentes mais relevantes em cada período, em coordenação com o Responsável de Sistemas.

- Determinar a categoria do sistema de acordo com o procedimento descrito no Anexo I do ENS e as medidas de segurança a aplicar em conformidade com as disposições do Anexo II do ENS.

- Verificar se as medidas de segurança são adequadas para a proteção da informação e dos serviços.

- Preparar os tópicos a discutir nas reuniões do Comité de Segurança, em coordenação com o Responsável de Sistema, fornecendo informação oportuna para a tomada de decisões.

- Responsável pela execução direta ou delegada das decisões da Direção, reunir-se-á com a Direção e o Responsável do Sistema, pelo menos uma vez por ano, para assegurar a estratégia.

Com respeito à documentação, e com base no Responsável do Sistema, estas são funções do Responsável pela Segurança:

- Propor a documentação de segurança de segundo nível (Normas de Segurança TIC -STIC- e Procedimentos Gerais do Sistema de Gestão de Segurança da Informação -SGSI-) à Direção e ao Responsável de Sistemas para a sua aprovação e assinar tal documentação.

- Aprovar a documentação de segurança de terceiro nível (Procedimentos Operacionais STIC e Instruções Técnicas STIC).

- Manter a documentação organizada e atualizada, gerindo os mecanismos de acesso à mesma.

Para o desenvolvimento de qualquer uma das suas funções, o Responsável pela Segurança poderá procurar a colaboração do Responsável de Sistema.

O Comité de Segurança da MHP assume as funções do Responsável pela Segurança.

8.6 Encarregado de Proteção de Dados

De acordo o indicado no RGPD e no LOPDGDD, o Ecarregado de Proteção de Dados terá pelo menos as seguintes funções:

- Informar e aconselhar o responsável pelo tratamento de dados e os seus funcionários das suas obrigações nos termos da RGPD e de outras disposições relativas à proteção de dados.

- Supervisionar o cumprimento das disposições do presente Regulamento, de outras disposições de proteção de dados da União ou dos Estados-Membros e das políticas do responsável pelo tratamento ou do subcontratante em matéria de proteção de dados pessoais, incluindo a atribuição de responsabilidades, a sensibilização e a formação do pessoal envolvido nas operações de tratamento, bem como as auditorias conexas.

- Prestar assessoria, conforme solicitado, sobre a avaliação do impacto da proteção de dados e controlar a sua aplicação em conformidade com o Artigo 35.

- Cooperar com a autoridade de controlo, neste caso a Agência Espanhola de Proteção de Dados.

- Atuar como ponto de contacto da autoridade de controlo para questões relacionadas com o tratamento, incluindo a consulta prévia referida no Artigo 36, e consultar, quando apropriado, sobre qualquer outro assunto.

A MHP nomeou um Encarregado de Proteção de Dados interno para a sua Organização.

8.7 Responsável de sistema

As funções do Responsável de Sistema são as seguintes:

- Desenvolver, operar e manter o sistema de informação durante todo o seu ciclo de vida, as suas especificações, instalação e verificação do seu bom funcionamento.

- Definir a topologia e o sistema de gestão do Sistema de Informação, estabelecendo os critérios de utilização e os serviços disponíveis no mesmo.

- Certificar-se de que as medidas de segurança específicas são devidamente integradas no quadro geral de segurança.

- Realizar exercícios e testes sobre os procedimentos operacionais de segurança e os planos de continuidade existentes.

- Monitorização do ciclo de vida dos sistemas: especificação, arquitetura, desenvolvimento, operação, alterações.

- Implementar as medidas necessárias para garantir a segurança do sistema durante todo o seu ciclo de vida, em conformidade com o Responsável pela Segurança.

- Aprovar qualquer modificação substancial na configuração de qualquer elemento do sistema.

- Suspender a manipulação de uma determinada informação ou a prestação de um serviço eletrónico se for informado de deficiências graves de segurança, após acordo com o Responsável pela Segurança e Direção.

- Realizar, com a colaboração do Responsável pela Segurança, as análises de risco necessárias, selecionar as salvaguardas a implementar e rever o processo de gestão de risco. Do mesmo modo, juntamente com o Responsável pela Segurança, aceitar os riscos residuais calculados na análise de riscos.

- Elaborar, em colaboração com o Responsável pela Segurança, a documentação de segurança de terceiro nível (Procedimentos Operacionais STIC e Instruções Técnicas STIC).

8.8 Comité de Segurança da Informação

Composto pelo Responsável pela Segurança, o Responsável de Sistema, o Encarregado de Proteção de Dados, e a direção, reúne-se pelo menos trimestralmente para coordenar a segurança da informação a nível da organização.

As suas funções são as seguintes:

- Atender às preocupações dos presentes em matéria de Segurança da Informação.
- Obter uma fotografia do estado de segurança da informação.
- Promover a melhoria contínua do SGSI.
- Elaborar a estratégia de evolução.
- Rever a Política, Normas e procedimentos pelo menos anualmente.
- Aprovar os requisitos de formação e sensibilização.
- Priorizar ações.
- Promover a execução das auditorias e técnicas do SGSI.
- Verificar se a Segurança da Informação está presente em todos os projetos.

9. Revisão e auditorias

O responsável pela segurança deve rever esta política anualmente ou quando ocorrerem alterações significativas que o aconselhem, e deve submetê-la novamente à aprovação da direção.

As revisões irão verificar a eficácia da política, avaliando os efeitos das mudanças tecnológicas e de negócio.

A direção será responsável pela aprovação das modificações necessárias ao texto quando ocorrer uma alteração que afete as situações de risco estabelecidas no presente documento.

O sistema de gestão de segurança deve ser auditado pelo menos anualmente, de acordo com um plano de auditoria desenvolvido pelo responsável pela segurança para as normas ISO 27001 (anual) e Esquema Nacional de Segurança (de dois em dois anos).

Serviço Integral de Gestão de Horários

mhp.pt info@mhp.pt +351 800 502 306

ESPANHA | PORTUGAL | REINO UNIDO| HOLANDA| ALEMANHA

ens Esquema Nacional de Seguridad ISO 27001 ISO 9001