Segurança da Informação e Confidencialidade

Departamento de IT

Ership
Grupo

Conceitos Prévios

Definições gerais de Segurança Informática

Segurança Informática

Refere-se aos sistemas que permitem a proteção das infraestruturas tecnológicas implantadas na organização (armazenamento, servidores, comunicações, etc..)

Segurança da Informação

Refere-se à proteção dos ativos de informação necessários para a organização.

Ativo de Informação

É tudo aquilo que na organização se considera importante e que pode conter informações como ficheiros, bases de dados, contas de utilizador, palavras-passe, e-mail, etc.

Fontes de Informação

São as origens que criam o ativo de informação como, por exemplo, OpycNet, Iris, um ficheiro anexado a um e-mail, Inca, ficheiros criados pelos utilizadores, etc.

SGSI

Sistema de Gestão de Segurança da Informação

Um Sistema de Gestão de Segurança da Informação (SGSI) é basicamente um conjunto de políticas de administração das informações, pretendendo proteger os seus ativos de informação essenciais para a continuidade do negócio.

O objetivo de um SGSI é implementar e monitorizar a segurança informática da organização, para que esta possa conseguir os seus objetivos comerciais e/ou de serviço.

Planear

Avaliam-se os riscos de segurança das informações e selecionam-se os controlos adequados

Fazer

Fase de implantação dos controlos definidos

Verificar

Rever e avaliar o correto funcionamento dos controlos definidos

Atuar

Fase em que são efetuadas alterações para manter os controlos definidos

Política Continuidade do Negócio

Um erro comum é pensar-se que o SGSI é uma questão meramente tecnológica e que só afeta o departamento de IT.

O SGSI é uma diretiva de alta direção para garantir o ciclo de vida da organização e que temos que respeitar e impulsionar todas as pessoas que trabalham na organização.

Toda a organização se deve envolver na tomada das medidas necessárias para garantir a segurança das informações e a segurança informática.

A informação é poder e é necessário ter procedimentos definidos para se garantir o seu acesso e disponibilidade. Esta informação é normalmente definida como valiosa, crítica ou Sensível.

Toda a informação tem caráter confidencial, pelo que é necessário estabelecer mecanismos de acesso a utilizadores para se evitar um acesso indevido.

A função do departamento de IT é tornar realidade todas as medidas necessárias para garantir a continuidade do negócio e traça normas de comportamento que têm que ser assumidas e apoiadas por todos os integrantes da organização.

Protocolo Segurança da Informação

Estratégia de empresa a longo prazo para se evitarem riscos derivados da falta de segurança nas informações na execução das decisões de negócio.

Este Protocolo de Segurança da Informação, anexo a esta formação, faz parte do Sistema de Cumprimento Normativo do Grupo e é aplicável em todas as sociedades que compõem o Grupo Ership.

As normas são de cumprimento obrigatório por todos os trabalhadores do Grupo Ership, independentemente do seu nível hierárquico

- Não se destruirá, alterará ou inutilizará de forma nenhuma a informação relevante.
- Não se enviarão mensagens qualificadas como SPAM a partir de meios proporcionados pelo grupo Ership.
- Não se instalarão nem descarregarão programas informáticos sem o prévio conhecimento do departamento de IT.
- Não se enviará informação sensível a nenhum terceiro sem o conhecimento prévio do responsável.
- Não se utilizará o e-mail do grupo Ership para o envio ou a receção de dados alheios aos trabalhos do posto de trabalho.
- Não se abrirão documentos anexos ou ligações em e-mails sem se verificar o remetente. Em caso de dúvida num e-mail suspeito, deve-se contactar a área de Sistemas do departamento de IT.
- Ter-se-á um cuidado especial com e-mails em que nos informem sobre uma alteração nas condições comerciais (alterações conta corrente) dos nossos fornecedores/clientes. Face a qualquer alteração, contactar telefonicamente o terceiro para confirmar a informação.
- As credenciais de acesso aos sistemas informáticos são únicas e intransmissíveis.
- Não conceder o controlo remoto do equipamento a nenhum terceiro sem aprovação prévia do departamento de IT.

Proteção da Informação

Tendo por objetivo garantir a proteção das informações do Grupo, durante o processo de contratação todos os trabalhadores subscrevem um compromisso de confidencialidade que contempla os pontos seguintes:

- Todo o pessoal do Grupo tem a obrigação de confidencialidade e dever de sigilo. Não se podem revelar, a uma pessoa alheia à organização, seja a que pretexto for, informações ou documentação a que tenham tido acesso no desempenho das suas funções, sem a devida autorização por escrito.

- Só é permitida a utilização da informação referida na secção anterior na forma exigida pelo desempenho das suas funções na empresa, sem que seja permitido dispor dela de qualquer outra forma ou para outra finalidade diferente.

- É proibido utilizar os recursos do Grupo, aos quais tenha acesso, para qualquer outra finalidade diferente das estritamente laborais. A Direção do Grupo reserva-se o direito de rever o e-mail do pessoal, as sessões de acesso à Internet, ou o uso de qualquer recurso propriedade do Grupo, quando se tiverem dúvidas razoáveis quanto ao seu uso inapropriado.

- Deve-se trabalhar sempre no sistema de informação autorizado, com os recursos e autorizações concedidos para que toda a atividade fique registada. Qualquer ficheiro criado fora do sistema de informação estabelecido, por exemplo, no ambiente de trabalho do seu computador ou mediante ficheiros temporários, deverá ser eliminado quando terminar a finalidade para a qual foi criado.

- Não se atenderão pedidos de informação por telefone (exceto nos casos autorizados com perguntas de segurança) e sem a devida identificação. Como regra geral, só são autorizados os pedidos de informação por escrito.

- A saída de suportes informáticos, computadores portáteis ou qualquer documentação física para fora da organização, só será efetuada quando for estritamente necessário, mantendo continuamente a devida diligência relativamente à proteção dos ativos e informações que são propriedade do Grupo.

- Todos os compromissos anteriores devem ser mantidos, inclusivamente depois de extinta a relação laboral/comercial com o Grupo Ership.

Protocolo Segurança Informática

Estratégia de empresa a longo prazo para evitar riscos derivados da falta de segurança nos sistemas informáticos/infraestrutura na execução das decisões de negócio.

- O Grupo Ership dispõe de sistemas de segurança perimétrica (Firewall) que permite o controlo do tráfego para e a partir da Internet.
- O Grupo Ership dispõe de um serviço Anti-Spam para que o e-mail seja filtrado de Spam e de outros ataques informáticos.
- O Grupo Ership dispõe de um serviço de antivírus para a deteção e eliminação de vírus informáticos.
- O Grupo Ership dispõe de uma plataforma de cibersegurança (DarkTrace) que monitoriza constantemente todo o tráfego de dados e deteta comportamentos suspeitos, podendo tomar decisões autónomas ou a pedido que permitem que se corte o tráfego e se evitem problemas derivados.
- O Grupo Ership dispõe de um departamento interno (IT Sistemas) que está encarregado de gerir a segurança informática. É muito importante que, face a qualquer dúvida sobre e-mail suspeito, ficheiro estranho, etc. se contactem os mesmos para a sua supervisão.
- O Grupo Ership dispõe de políticas de Backup das informações que garantem a recuperação da mesma em situações concretas. É muito importante que os utilizadores armazenem a informação importante nos recursos de rede (Unidades U, G, etc.) que é a origem dos backups das informações. Estes Backups são efetuados a dados (ficheiros, e-mails, etc.) e também a sistemas.

O Utilizador … o elo mais fraco da cadeia!

No que se refere à segurança informática, o utilizador é o elo mais fraco. O utilizador, para evitar (ou minimizar) o risco de ataques informáticos, deve:

- Não descarregar ficheiros da Internet, nem visitar páginas web "desconhecidas".
- Não conectar dispositivos alheios aos equipamentos informáticos do Grupo.
- Não instalar por iniciativa própria nenhum produto informático em computadores e sistemas de informação da organização.
- Colocar-se as perguntas seguintes face a qualquer e-mail recebido:

  - Conheço o remetente?
  - Esperava o e-mail?
  - Reconheço o ficheiro anexo?

  Aplicar sempre o senso comum e, se recebermos algum e-mail estranho de um fornecedor/cliente, antes de mais nada, falar com o departamento de IT ou então com o terceiro.

E o que é mais importante, face a qualquer dúvida, consultar o departamento de IT, que existe para os ajudar!

ERSHIP Grupo
Lagasca, 88
28001 Madrid (Espanha)

+34 914 263 400
www.ership.com