Ership
Grupo

PROTOCOLO DE SEGURANÇA DA INFORMAÇÃO

Índice

INFORMAÇÃO, CONTROLO DE MODIFICAÇÕES E APROVAÇÃO

Informações importantes sobre este documento	
Identificação de Políticas	Política de Segurança da Informação
Política de execução global ou nacional	Global
Secção de outras políticas que desenvolve	
Regras que substitui	N/A
Regras que revoga	Tudo o que está acima no mesmo assunto
Regras relacionadas	Código de Ética Código de Conduta
Unidade de negócio ou função que afeta	Todos
Pessoal afetado	Todos
Principal responsável pela sua vigilância	Unidade de Conformidade

O presente Protocolo será revisto quando forem detetadas situações que aconselhem a atualização do seu conteúdo e, em seguida, produzida uma nova versão do mesmo.

Nome do arquivo	Versão	Resumo das Alterações	Autor	Data

O presente protocolo foi aprovado pelas seguintes pessoas nas datas a seguir indicadas.

Número	Departamento	Cargo	Empresa	Data

INTRODUÇÃO

Numa economia globalizada como a atual, a ciência da computação e os meios telemáticos adquiriram um papel essencial no desenvolvimento de negócios de qualquer operador económico. Especialmente no Grupo ERSHIP, presente em mais de 40 portos em todo o mundo, os meios de comunicação informáticos não são apenas uma ferramenta, mas já uma necessidade.

E com as muitas vantagens da informatização da atividade económica surgem também algumas fragilidades que todas as empresas com um determinado compromisso ético devem prevenir e reduzir.

Por um lado, existem os chamados crimes informáticos *lato sensu*, entre os quais se encontram os comportamentos que consistem em deteriorar, alterar ou eliminar, entre outros, os programas informáticos ou documentos eletrónicos de outros, bem como tornar os dados informáticos inacessíveis sem serem autorizados a fazê-lo. Mas não só, porque os meios de comunicação informáticos podem levar à possibilidade de descobrir ilicitamente segredos ou violar a privacidade de outro, sem o seu consentimento, práticas todas rejeitadas pela cultura empresarial empenhada que define A ERSHIP.

Mas, por outro lado, o Grupo também pode ser vítima de tal cibercrime. E-mails de spam, *fishing* e *malware* como anexos a um e-mail inofensivo são algumas das formas mais comuns de ser prejudicado por qualquer um destes tipos criminosos.

É por isso que, através deste protocolo, a ERSHIP pretende implementar uma série de medidas, controlos e procedimentos destinados a prevenir e evitar a prática de crimes informáticos, bem como minimizar o risco de serem vítimas deles e neutralizar as consequências negativas que estas poderiam ter no Grupo.

CAPÍTULO I. ASPETOS GERAIS

ARTIGO 1. FINALIDADE DO PRESENTE PROTOCOLO

1 - A estratégia de luta para garantir a segurança da informação da Empresa consiste principalmente em garantir o cumprimento dos regulamentos aplicáveis e em assegurar uma coordenação adequada das práticas no negócio seguida pelas empresas do Grupo, tudo isto no quadro da consecução do interesse da proteção da privacidade pessoal e da segurança informática nos negócios e do apoio a uma estratégia de negócio para a longo prazo que evite riscos derivados da falta de segurança na informação na execução de decisões empresariais.

2. Para o efeito, a Empresa tem em conta todos os interesses legítimos que convergem na sua atividade.

ARTIGO 2. ÂMBITO DE APLICAÇÃO E DE SUJEITOS OBRIGATÓRIOS

1. O presente Protocolo de Segurança da Informação é aplicável em todas as empresas que compõem o Grupo, bem como nas empresas investidas não integradas no Grupo sobre o qual a Empresa tem controlo efetivo, dentro dos limites legalmente estabelecidos.

2. As suas regras devem ser respeitadas por todos os profissionais do Grupo, independentemente do seu nível hierárquico, da sua localização geográfica ou funcional e da empresa do Grupo para a qual prestam os seus serviços.

3. Para efeitos do presente protocolo, os Acionistas, Membros do Conselho de Administração, Administradores e Colaboradores de todas as sociedades e entidades que o compõem, bem como as outras pessoas cuja atividade está expressamente sujeita a este protocolo, são considerados Sujeitos Obrigados.

4. Nas organizações e entidades em que o Grupo, sem participação maioritária, é responsável pela gestão, os profissionais que representam o Grupo promoverão a aplicação do presente Código.

5. Além disso, o presente Protocolo de Segurança da Informação é igualmente aplicável, se for caso disso, às empresas contratadas que atuam em nome da Empresa, bem como a *joint ventures, sindicatos* temporários de empresas e outras associações equivalentes, quando a Empresa assume a sua gestão.

6. A sua aplicação será adaptada aos regulamentos sectoriais de cada uma das áreas de atividade da ERSHIP.

ARTIGO 3º. EXCEÇÕES

Com exceção dos expressamente previstos na sua redação, o presente protocolo não prevê exceções à sua devida aplicação por todos os Sujeitos Obrigados.

CAPÍTULO II. PRINCÍPIOS E CONDUTAS PROIBIDAS

ARTIGO 4º. PRINCÍPIOS E OBJETIVOS

1. Através do presente documento, a ERSHIP proclama a sua vontade de cumprir os regulamentos que regem o sector das telecomunicações. Este texto está configurado com o objetivo de dotar o pessoal da Ership de orientações adequadas para a conduta em relação aos diferentes meios e meios digitais de conformidade obrigatória.

2. O Protocolo desenvolve o compromisso adquirido pela ERSHIP de agir de acordo com a legislação aplicável para cada um dos sectores de atividade em que intervém, bem como a responsabilidade ética de proteger os direitos à privacidade do seu próprio pessoal e de terceiros que possam estar relacionados com o Grupo.

3. A ERSHIP opõe-se à utilização de meios informáticos para fins ilegais. Trata-se não só de conduta criminosa, mas de qualquer conduta que possa ser considerada ilegal, quer seja cometida contra ou em benefício do próprio Grupo, do seu pessoal ou de qualquer terceiro.

ARTIGO 5º. CONDUTA PROIBIDA

1. Os dados, programas ou documentos eletrónicos pertencentes à ERSHIP ou a terceiros não devem ser destruídos, alterados, tornados inúteis ou danificados sem o consentimento expresso de uma pessoa competente.

2. O acesso de outros utilizadores à rede não deve ser intencionalmente impedido.

3. As mensagens qualificadas como *spam* não serão enviados através dos meios informáticos fornecidos pela ERSHIP.

4. Nenhum programa ou aplicações que causem, ou sejam suscetíveis de causar, qualquer tipo de alteração nos sistemas informáticos detidos pela ERSHIP ou por terceiros serão intencionalmente introduzidos.

5. Não serão introduzidos, descarregados da Internet, reproduzindo, utilizando ou distribuindo programas informáticos não expressamente autorizados pela ERSHIP, ou qualquer outro tipo de trabalho ou material cujos direitos de propriedade intelectual ou industrial pertençam a terceiros e a correspondente licença ou autorização não esteja disponível para o mesmo.

6. Não devem ser instaladas cópias ilegais de qualquer programa informático, incluindo programas corporativos.

7. Qualquer dos programas de computador legalmente e devidamente instalados pelo Departamento de IT não será removido.

8. O conteúdo obsceno, imoral, ofensivo ou qualquer outro conteúdo que não esteja de acordo com o trabalho realizado pela Ership não será descarregado, reproduzido, armazenado ou enviado a partir dos efeitos informáticos da ERSHIP.

9. As páginas web expressamente proibidas pelo Departamento de IT não serão acedidas de forma fraudulenta.

10. Informações confidenciais ou sensíveis não serão enviadas por e-mail, se não for estritamente necessária.

11. O e-mail corporativo não será utilizado para enviar ou receber dados pessoais fora do trabalho da ERSHIP.

12. Não serão abertos anexos ou links sem verificar o remetente e o conteúdo do e-mail e, em todo o caso, sem prosseguir de acordo com o procedimento de controlo desenvolvido neste Protocolo.

CAPÍTULO III. MEDIDAS PREVENTIVAS E DE CONTROLO

ARTIGO 6º. IDENTIFICAÇÃO DO UTILIZADOR

1. O Departamento de IT estabelecerá um sistema de identificação e autenticação dos utilizadores e gestão das credenciais dos utilizadores para cada uma das finalidades do computador corporativo, de forma a poder identificar o utilizador que faz todo o uso do efeito em todos os momentos.

2. As palavras-passe para a identificação dos utilizadores da ERSHIP devem ser robustas e alteradas pelo menos uma vez por ano.

ARTIGO 7º. LICENÇAS DE UTILIZAÇÃO

O Departamento de IT estabelecerá um inventário de licenças de software que manterá continuamente atualizado.

ARTIGO 8º. ACESSO PROIBIDO

O Departamento de IT, através do seu fornecedor antivírus, gere um tipo de páginas web que, quer por considerarem o seu conteúdo obsceno, imoral ou ofensivo, quer porque entendem que o seu acesso é contrário aos valores éticos da ERSHIP, serão entendidas como proibidas. O Departamento de IT através de uma firewall impede o acesso a estas páginas web a partir de sistemas informáticos corporativos, e pode extraordinariamente e com autorização, desbloquear temporariamente um destes sites.

ARTIGO 9º. MEDIDAS DE CONTROLO CONTRA *SPAM*, *FISHING* E E-MAILS COM ANEXOS SUSPEITOS

Para evitar que A ERSHIP sofra um ataque informático, o pessoal da ERSHIP deve agir fazendo três perguntas antes de qualquer e-

mail recebido para o endereço de e-mail corporativo:

a) Conheço o remetente? Se o remetente não for conhecido, é provável que tenha de descartar o e-mail recebido.
b) Estava à espera do correio? Se for de um remetente conhecido, mas tal e-mail não era esperado, deve ser exercida alguma cautela quanto ao conteúdo que esse e-mail lhe pede e ainda mais sobre os ficheiros que o e-mail anexa.
c) Reconhece o arquivo em anexo? No caso de descarregar o anexo de um e-mail, deve digitalizá-lo com o software *anti-malware* autorizado pelo Departamento de IT antes de o abrir. Em caso de dúvida, apague o ficheiro.

Além disso, estas situações devem ser sempre chamadas ao conhecimento do Departamento de IT, de modo que ajam em conformidade e lhes deem o devido acompanhamento.

CAPÍTULO IV. MONITORIZAÇÃO, CONTROLO E PROCEDIMENTO

ARTIGO10º. DEVER DE COMUNICAR POSSÍVEIS DANOS INFORMÁTICOS

1. Quando qualquer membro do pessoal da ERSHIP suspeitar que foi vítima de *fishing* ou descarregou um anexo que se revelou ser, ou suspeita que pode ser malware, informarão imediatamente o Departamento de IT, mesmo antes de detetarem comportamentos anormais pelo efeito do computador.

2. Pode também dirigir-se diretamente aos membros da Unidade de Conformidade ou poderá fazê-lo através do Canal de Reclamações.

3. Em todo o caso, a ERSHIP garantirá a confidencialidade da denúncia e os dados do autor da denúncia, bem como a indemnização do autor da denúncia de boa-fé.

4. Em caso de dúvida ou dúvidas sobre o conteúdo deste protocolo ou se não tiver a certeza de como aplicá-lo em determinados casos, os Sujeitos Obrigados podem contactar a Unidade de Conformidade da ERSHIP através dos meios acima referidos.

ARTIGO11º. IMPACTO DAS INVESTIGAÇÕES INTERNAS NA GESTÃO DA INFORMAÇÃO

1. Os efeitos corporativos da ERSHIP são sempre propriedade da mesma, independentemente do utilizador a quem são emprestados, e devem ser utilizados de acordo com a atividade económica e os valores éticos subscritos pelo Grupo.

2. O princípio da transparência impõe a necessidade de a Unidade de Conformidade poder efetuar as inspeções correspondentes nos efeitos de IT das empresas.

3. A utilização de efeitos informáticos corporativos implica a aceitação, pelo utilizador, da possibilidade de a Unidade de Conformidade, no âmbito de uma investigação interna, poder aceder a este efeito e despejar as informações que contém e ser considerada necessária para o bom final do inquérito.

4. No âmbito de uma investigação interna, a Unidade de Conformidade pode autorizar o acesso a qualquer computador, tablets, telemóveis e quaisquer outros aparelhos informáticos corporativos, a fim de recolher as informações necessárias para a realização bem-sucedida do inquérito. Esse acesso deve ser proporcionado para efeitos do inquérito e limitar-se apenas ao conteúdo que possa incluir as informações

solicitadas, não sendo possível um acesso curioso. As informações obtidas em consequência desse acesso serão confidenciais.

5. No âmbito de uma investigação interna, a Unidade de Conformidade pode autorizar o acesso ao e-mail corporativo de qualquer utilizador para recolher as informações necessárias para a conclusão bem-sucedida do inquérito. Esse acesso deve ser proporcionado para efeitos do inquérito e limitar-se apenas ao conteúdo que possa incluir as informações solicitadas, não sendo possível um acesso curioso. As informações obtidas em consequência desse acesso serão confidenciais.

ARTIGO 12. REGIME SANCIONATÓRIO

1. Em caso de violação por qualquer sujeito obrigado, a ERSHIP aplicará o regime sancionatório previsto no Código de Conduta, em conformidade com a gravidade da violação e no quadro jurídico aplicável na jurisdição em que foi cometido. Da mesma forma, A ERSHIP informará as autoridades competentes da violação regulamentar se houver indícios de crime.

2. A Unidade de Conformidade coordenará:

a) Com o Departamento de Recursos Humanos as ações que são necessárias para adotar em relação ao pessoal da ERSHIP.
b) Com o Departamento Jurídico da ERSHIP aqueles que são aplicáveis a pessoas associadas à ERSHIP por relação comercial.

3. Em ambos os casos, a Unidade de Conformidade informará imediatamente o Conselho de Administração, sempre que a gravidade dos casos o justifique.

4. Em todo o caso, as medidas adotadas devem respeitar o princípio da proporcionalidade e o interessado será ouvido de modo que possa dar conta do sucedido.

ARTIGO 13.º. REVISÃO DOS RESULTADOS

1. A ERSHIP revirá periodicamente a sua política de segurança da informação, em especial o grau de conformidade com as ações iniciadas de acordo com o programa estabelecido, os seus resultados e a legislação aplicável.

2. Para a revisão do grau de conformidade em segurança da informação, devem ser tomados em consideração, pelo menos, os seguintes fatores:

a) Queixas externas.
b) Sugestões internas.
c) Ações de empresas concorrentes.
d) Comentários ao cliente.
e) Legislação futura.
f) Planos sectoriais.
g) Novas tecnologias aplicáveis ao sector de atividade da empresa de acordo com o seu propósito corporativo.

ARTIGO 14.º. MONITORIZAÇÃO E CONTROLO

1. As empresas do grupo adotarão os mecanismos de controlo necessários para assegurar, no âmbito de uma segurança adequada das informações, o cumprimento dos regulamentos. Devem igualmente dedicar recursos humanos e materiais adequados e suficientemente qualificados a esses fins.

2. Anualmente, a Unidade de Conformidade, em coordenação com o Departamento de IT, apresentará um relatório sobre o grau de conformidade com o Protocolo de Segurança da Informação.

ARTIGO 15.º. MONITORIZAÇÃO

1. Para assegurar o cumprimento contínuo dos procedimentos desenvolvidos no presente protocolo, A ERSHIP procederá a revisões internas e periódicas, emitindo os correspondentes relatórios de conclusões, que serão avaliados pela Unidade de Conformidade, a fim de apresentar um relatório ao Conselho de Administração.

2. Esses relatórios mencionarão expressamente as deficiências identificadas durante o reexame e elaborarão planos de ação para as remediar.

3. A periodicidade desta revisão interna será estabelecida seguindo critérios objetivos para assegurar o cumprimento regulamentar.

4. A Unidade de Conformidade deve manter um registo atualizado de quaisquer infrações que lhe sejam efetuadas, bem como das ações contra elas tomadas.

5. No caso de, após a denúncia e investigação correspondentes, se detetar que a violação das disposições aqui contidas resultou de um defeito nos atritos ou controlos implementados pela ERSHIP, será revisto e atualizado a fim de evitar que sejam reproduzidos no futuro.

CAPÍTULO V. CONSIDERAÇÕES ADICIONAIS

ARTIGO 16.º. CONHECIMENTO DA LEGISLAÇÃO

1. A empresa tem a obrigação de conhecer toda a legislação que lhe é aplicável e as potenciais consequências do seu incumprimento.

2. Os requisitos legais aplicáveis serão permanentemente atualizados para evitar o risco de incumprimento de novas regulamentações em matéria de segurança da informação que possam surgir após a aprovação e aplicação do presente protocolo.

ARTIGO 17.º. DIFUSÃO

1. A ERSHIP estabelecerá as medidas adequadas para garantir que os trabalhadores, gestores e membros do Conselho de Administração estejam cientes dos requisitos decorrentes dos regulamentos relativos à segurança da informação. Estas medidas incluem a organização de planos de formação e cursos de formação especiais que, dirigidos ao pessoal em geral e especificamente às pessoas que desempenham esses trabalhos, que, devido às suas características, são adequados para detetar os factos e operações que possam estar relacionados com comportamentos de risco para a segurança da informação, formar todo o pessoal para realizar tal deteção e saber como proceder nesses casos.

2. O presente protocolo será entregue ao pessoal da ERSHIP que, devido à sua atividade, possa incorrer em alguns dos riscos descritos.

3. No caso das pessoas que são membros da Empresa, será função destas assegurar aos novos membros da empresa que estes conhecem tanto o Código de Conduta da ERSHIP como o presente Protocolo, estando alinhados e respeitando o conteúdo de ambos os textos.

4 - A Unidade de Conformidade assegurará que os Sujeitos Obrigados tenham acesso ao presente Protocolo, promovendo as medidas necessárias para tornar o seu conteúdo facilmente acessível e resolver qualquer dúvida que o pessoal, funcionários, gestores, diretores ou membros da ERSHIP possam levantar relativamente ao seu conteúdo e âmbito.

ARTIGO 18.º. FORMAÇÃO

Cabe ao Departamento de Recursos Humanos promover a formação recorrente entre o pessoal da ERSHIP, garantindo que todos os sujeitos vinculados ao presente Protocolo realizem e aproveitem a formação à sua disposição.

ARTIGO 19.º. REVISÃO DO PROTOCOLO SOBRE A SEGURANÇA DA INFORMAÇÃO

1. O presente protocolo deve ser permanentemente atualizado.

2. O seguinte é motivo de atualização do protocolo:

a) Mudanças no ambiente legislativo.

b) Adaptação a políticas, recomendações ou normas estabelecidas pela ERSHIP.

c) Introdução de todas as alterações necessárias para melhorar a operação de prevenção derivada dos desenvolvimentos e boas práticas observadas no sector ou da análise dos pontos de melhoria identificados pela Unidade de Conformidade ou pelo Departamento de IT.

3. Sob a responsabilidade da Unidade de Conformidade, deve ser mantido um registo de alterações ao protocolo. Esse registo incluirá uma indicação sumária das alterações efetuadas, as razões pelas quais essas alterações foram efetuadas e as datas em que foram efetuadas.

4. As alterações ao Protocolo que possam ser necessárias em resultado do procedimento de atualização serão efetuadas pela Unidade de Conformidade da Ership.

5. Uma vez efetuadas as alterações, o Protocolo será disponibilizado a todos os Sujeitos Obrigados.