Partner
in Payments

Manual de Segurança de Informação (externo)

Versão: 02.07

Data: 2019-04-22

Estado: Final

Classificação: Restrito

Nível: 3 - Operacional

Tema: Segurança

Referência: DCSIBS180168

Signature Not Verified
Digitally signed by Gestao Documental - SIBS
Date: 2019.04.23 16:05:58 +01:00
Reason: Controlo de Qualidade
Location: SIBS

Ficha Técnica

Referência:	DCSIBS180168
Título do Documento:	Manual de Segurança de Informação (externo)
Versão:	02.07
Estado:	Final
Classificação:	Restrito
Tipo do Documento:	Norma de Segurança
Nível:	3 - Operacional
Tema	Segurança
Área Funcional Responsável:	AF Segurança

Lista de Distribuição

Nome
Colaboradores externos, consultores e prestadores de serviços do Grupo SIBS, Clientes do Grupo SIBS.

Revisões

Versão	Data	Descrição	Autor
01.00	2001-12-31	Primeira versão do documento (Não publicada)	Gabinete de Auditoria e Qualidade Dep. de Certificação e Segurança Dep. de Produção
02.00	2013-04-09	*Major revision* (Não publicada) O âmbito do documento foi refocado, tendo sido eliminados todos os conteúdos que eram específicos de determinadas atividades e que estão expressos em políticas específicas, ficando o manual como um guia essencial da segurança na SIBS. Atualização e introdução de conceitos e procedimentos.	AF Segurança
02.01	2014-05-13	*Minor revision* (Não publicada) Revisão editorial para eliminar os elementos (como nomes de colaboradores) que não eram apropriados para a distribuição do documento para fora do Grupo e para incluir referência que existe uma versão em Inglês.	AF Segurança
02.02	2018-01-24	*Minor revision* (Não publicada) • Alinhamento das referências a Áreas Funcionais com versões mais recentes da estrutura da empresa; • Correções e melhorias editoriais diversas.	AF Segurança
02.03	2018-03-20	Inclusão de referência ao princípio de *least privilege*. Reforço de regras sobre partilha de informação intragrupo. (Versão Não publicada)	AF Segurança
02.04	2018-05-29	*Minor revision* Revisão editorial para criação de versão interna e externa do documento, alteração da lista de distribuição e inclusão das referências dos documentos.	AF Segurança
02.05	2018-11-12	*Minor revision* Preparação para inclusão em contratos com a remoção das referências a documentos internos constantes do Sistema de Gestão de Segurança de Informação. Adequação do *template* para o *layout* da SGPS. Correções e melhorias editoriais diversas.	AF Segurança
02.06	2019-03-21	Substituição do LOGO da Empresa	AF Qualidade

Versão	Data	Descrição	Autor
02.07	2019-04-22	*Minor revision* Alargamento da audiência do manual com a inclusão na lista de distribuição de "Clientes do Grupo SIBS": • Alinhamento com o Manual de Segurança – Boas práticas de Segurança em Acordos e Contratos; • Observância da recomendação emanada da Auditoria Interna ISO 9001 e 20000.	AF Segurança

Índice

1 Introdução

1.1 Objetivo

Este documento tem como objetivo apresentar uma visão global (um resumo), das principais regras e recomendações destinadas a proteger os recursos de informação do Grupo SIBS, que se aplicam à generalidade dos indivíduos que acedem, processam ou criam informação institucional, ou interagem com os sistemas e infraestruturas tecnológicas associadas a essa informação.

Este documento deve ser distribuído a todos os indivíduos que acedem, processam ou criam informação institucional, independentemente da sua relação com o Grupo SIBS. Excetua-se o público em geral que tem apenas acessos de consulta a informação classificada como “Pública”.

Este documento não substitui o restante normativo de segurança SIBS ou a legislação em vigor, nomeadamente quando estes possam ser mais restritivos nas práticas ou mais específicos nos temas abordados.

O normativo de segurança SIBS está disponível para consulta na área de normativos do IntraSIBS e deve ser consultado e compreendido pelos colaboradores à medida das suas necessidades.

Este manual está disponível em versão de distribuição interna (DCSIBS130051), versão externa em língua portuguesa (DCSIBS180168) e versão externa em língua inglesa (DCSIBS140152).

1.2 Âmbito

O presente Manual aplica-se a todos os aspetos da Segurança de Informação do Grupo SIBS com exceção dos aspetos relacionados com segurança física.

1.3 Referências

- ISO/IEC 20000 – Gestão de Serviços IT.

1.4 Definições

Termo	Definição
Credenciais de acesso	As credenciais de acesso são os elementos que comprovam a identidade de quem se apresenta perante um sistema ou perante uma aplicação para a ela tentar aceder. O comprovativo da identidade é feito após validação com sucesso da credencial disponibilizada. As credenciais de acesso podem assumir uma ou mais das seguintes formas: • Algo que se possua, ex.: um cartão magnético/*chip*, uma chave física; • Algo que se saiba, ex.: uma senha, um código secreto, informação pessoal; • Algo que se seja, ex.: caraterísticas biométricas, como impressão digital ou imagem da retina.

Termo	Definição
Fingerprint	Código de identificação digital que permite identificar univocamente um ficheiro. É utilizado para validar que um ficheiro (para instalação de *Software*, por exemplo) potencialmente obtido por via insegura (descarregado da *Internet*, por exemplo) se encontra integro e corresponde ao ficheiro original. Tipicamente os *fingerprints* são produzidos por aplicação de uma função criptográfica irreversível (por exemplo *hash* usando uma função SHA-1 ou MD5) no ficheiro que se pretende identificar, sendo o *fingerprint* distribuído por um canal seguro, distinto do canal de distribuição do ficheiro. Para validação do *fingerprint*, aplica-se no ficheiro a validar a função de geração do *fingerprint* e confirma-se o resultado da função com o *fingerprint* recebido.
Incidente de segurança	Define-se como incidente de segurança de informação qualquer evento que, comprovadamente, origine perda de: • Integridade; • Confidencialidade; • Disponibilidade de recursos de informação da SIBS. No caso da disponibilidade consideram-se apenas os eventos resultantes de incumprimento/violação de obrigação.
Informação institucional	Toda a informação, independentemente do seu conteúdo ou formato, que for criada ou usada no âmbito da atividade do Grupo SIBS.
Least Privilege	Princípio de segurança que significa que a cada utilizador, programa ou processo, apenas devem ser concedidos a informação ou recursos estritamente necessários à persecução do seu objetivo legítimo.
Need to know	Princípio de segurança que significa que só deve ter conhecimento/acesso a um bem (e.g., informação, sistema, espaço físico) quem dele necessite para exercício das suas funções.
Passphrase	Senha de acesso de grandes dimensões.
Segurança de informação	A segurança da informação consiste na proteção dos dados e outras informações, e dos sistemas, aplicações e funções e infraestruturas utilizadas na criação, processamento ou guarda de informação de modo a evitar a sua disseminação, modificação, destruição ou indisponibilização acidental ou criminosa, assegurando assim a confidencialidade, integridade e disponibilidade.
Software malicioso	*Software* desenvolvido com o objetivo de infiltração e execução de código sem o conhecimento e consentimento do responsável pelo sistema atacado com intuito de prejudicar alguém e/ou obter algum tipo de vantagem.
Utilizador	Conceito utilizado nos acessos lógicos para representar uma entidade (física/informática) num sistema ou aplicação. As entidades físicas podem ser: • Colaboradores ou outras pessoas com necessidade de acesso; • Grupos funcionais; • Sistemas ou aplicações.

2 Manual de segurança

2.1 Segurança de informação

1. A informação institucional é um bem do Grupo SIBS e como tal deverá ser protegida desde o momento da sua criação e durante a sua vida útil, até à sua eliminação autorizada.
2. A segurança da informação institucional é uma responsabilidade de todos, e pretende assegurar que é mantida íntegra e que se encontra sempre disponível para ser utilizada, apenas e só, pelos elementos autorizados para o efeito.
3. A informação institucional não deve ser do conhecimento ou estar na posse de apenas um indivíduo, sem que existam outras salvaguardas de integridade / disponibilidade.
4. Os utilizadores devem utilizar os vários repositórios à sua disposição para salvaguarda da informação institucional que manipulam[i]. Estes repositórios asseguram, dentro de certos limites técnicos, a salvaguarda e capacidade de reposição de versões anteriores da informação aí armazenada. A informação criada e processada no âmbito dos serviços prestados pelo Grupo tem armazenamento e salvaguardas específicos para o efeito e distintos dos anteriores.
5. A informação deve ser classificada de acordo com a sua confidencialidade, períodos de retenção e necessidade de acesso de colaboradores ou outro pessoal autorizado. A classificação da informação é, tipicamente, uma responsabilidade de quem a cria ou recebe (de terceiros).
6. A classificação da informação e correspondente proteção, baseiam-se no valor intrínseco da informação para o Grupo, tendo em conta os riscos estimados provenientes da perda (permanente ou temporária), adulteração ou disseminação não autorizada dessa informação. Salienta-se que:
    - Deve haver especial cuidado na proteção de toda a informação não pública que possa ser transportada ou comunicada para fora das instalações físicas da SIBS;
    - Em caso algum poderão ser partilhadas com terceiros, incluindo entre empresas do próprio Grupo SIBS, informações de carácter comercial e/ou de negócio sobre a respetiva clientela, incluindo eventuais dados ou elementos suscetíveis de criar na parte destinatária uma vantagem negocial ou competitiva por acesso a qualquer informação privilegiada. De modo particular, esta disposição afeta os diversos operadores de *acquiring* servidos pela SIBS enquanto processador, onde se inclui a SIBS Pagamentos;

[i] São exemplos desses repositórios de informação institucional: os *fileshares* departamentais, os *fileshares* de utilização partilhada ou os *sites* do IntraSIBS.

- Devem ser respeitados os prazos de salvaguarda[ii] da informação que tenha valor como comprovativo legal, fiscal ou interno (de auditoria);
- A proteção da informação deve ter em consideração todos os formatos em que esta pode ser comunicada, processada e armazenada[iii].

7. Do ponto de vista de confidencialidade a informação institucional deve ser classificada num dos seguintes níveis:

- **Pública**: Informação que pela sua natureza não requer medidas especiais de acesso, manuseamento, disseminação, armazenamento e destruição. É relacionada com interesses de negócio ou da comunidade e não se refere a uma pessoa ou grupo em particular;
- **Restrita**: Informação recebida, mantida ou pertencente à SIBS e que deve ser restrita a pessoas ou grupos autorizados, uma vez que a sua disseminação poderia dar vantagens injustas a um indivíduo ou a uma organização em ambiente competitivo, ou constituir infração contratual. Esta informação requer medidas de segurança moderadas, mas seletivas quanto ao acesso, manuseamento, disseminação, armazenamento e destruição. Por omissão, toda a informação sem indicação explícita da sua classificação de segurança é considerada como "Restrita";
- **Confidencial**: Informação que é criada por, ou confiada à SIBS para seu uso confidencial e só deverá ser disponibilizada a elementos autorizados. Esta informação não deverá ter uma divulgação generalizada, uma vez que a sua disseminação não autorizada poderá ser prejudicial ou ilegal. Esta informação requer máximas salvaguardas administrativas ou tecnológicas para o acesso, manuseamento, disseminação, armazenamento e destruição;
- **Secreta**: Informação com as mesmas caraterísticas da informação confidencial, embora não possa ser do conhecimento total por um único indivíduo. A sua existência em claro (não dissimulada) só poderá ter lugar dentro de dispositivos criptográficos seguros.

2.2 Controlo de acessos[iv]

1. A cada pessoa só devem ser disponibilizados os acessos e os privilégios necessários ao exercício das funções que lhe estão confiadas (princípios de *need to know* e *least privilege*).

2. Os acessos lógicos estão sujeitos a um processo[v] de solicitação, escrutínio e aprovação prévio à sua disponibilização, alteração e remoção.

[ii] Tipicamente, 10 anos para documentos fiscais e 7 anos para os restantes.

[iii] Por exemplo de forma eletrónica, em papel, por telefone, por *fax*, etc.

[iv] Com as devidas adaptações, o descrito nesta secção aplica-se da mesma forma aos acessos de grupos de pessoas e aos acessos para sistemas e aplicações.

3. Cada indivíduo é responsável pelas ações que realiza com os acessos que lhes são disponibilizados e pela salvaguarda da informação a que acede.
4. Os acessos a recursos de informação e as ações realizadas sobre, ou nesses recursos, são controlados de forma a permitir:
    - a associação entre as ações realizadas e os agentes que realizam esses acessos;
    - a implementação dos princípios de *need to know* e *least privilege*; e
    - a prevenção ou deteção de situações anómalas que possam comprometer a Segurança de Informação.
5. A cada pessoa com necessidade de acesso a informação, é atribuído (nos sistemas, aplicações e repositórios de informação), um ou mais utilizadores nominais que a representam durante os acessos e ações aí realizadas, bem como as respetivas credenciais de acesso.
6. Os utilizadores e as suas credenciais de acesso são de utilização pessoal e intransmissível. Compete a cada indivíduo a proteção dos elementos de acesso que lhe são confiados: ex. não os divulgando e memorizando-os / registando-os de forma segura.
7. As permissões de acesso devem ser retiradas assim que deixem de ser necessárias para a execução de funções.
8. É responsabilidade de cada utilizador:
    - Declarar e solicitar a correção de situações em que detete a existência de acessos excessivos para a execução das suas funções[vi],
    - Reportar como incidente de segurança a utilização ou tentativa de utilização indevida dos seus acessos.
9. Um utilizador, poderá ver os direitos de acesso aos sistemas de informação da SIBS suspensos, por motivos relacionados com a manutenção da sua segurança física, estado emocional ou o seu próprio bem-estar, ou por razões relacionadas com a preservação da segurança e do bem-estar de outros elementos, ou ainda, para a defesa de recursos ou objetivos de negócio do Grupo.

2.3 Senhas

Quando são utilizadas senhas como credenciais, deve ser respeitado o seguinte:

1. As senhas devem ser mantidas confidenciais para assegurar a sua efetividade.
2. O registo das senhas só é permitido se for feito de forma cifrada ou forem aplicados outros métodos equivalentes que garantam a sua confidencialidade.

[v] Gerido pelo *Helpdesk* Acessos Lógicos (acessos.logicos@sibs.pt).

[vi] Poderá suceder, por exemplo, porque o utilizador mudou de funções ou que lhe foram atribuídas permissões a mais.

3. As senhas devem ser definidas de modo a que não seja provável a sua suposição, seja por intermédio de experimentação, seja por suposição educada[vii].
4. Recomenda-se a utilização de mecanismos que facilitem a definição de senhas seguras. Por exemplo: a utilização de *passphrases* ou a concatenação aleatória de silabas para produzir uma senha legível e memorizável, mas que não corresponde a uma palavra existente.
5. Para impedir a reutilização / escalar de acessos no caso de comprometimento de senhas devem ser utilizadas senhas distintas para acesso a sistemas/informação com criticidade diferente[viii].
6. Sempre que suspeite que uma senha possa ter sido comprometida ou quando isso lhe for solicitado, o utilizador deve alterar a sua senha de acesso.

2.4 Instrumentos de trabalho

1. Os sistemas ou suportes informáticos colocados pela SIBS à disposição dos seus utilizadores são instrumentos de trabalho sob a responsabilidade pessoal desses utilizadores.
2. Cada utilizador deve ser parcimonioso, usando o mínimo dos instrumentos e recursos partilhados para assegurar as suas atividades e não colocando em causa a disponibilidade de recursos aos outros utilizadores.
3. Os utilizadores devem interagir com os sistemas que lhes são confiados de forma a prevenir a utilização desses sistemas de forma indevida ou por pessoal não autorizado. Por exemplo: desligando ou bloqueando sessões nos sistemas quando estes não estão em utilização e, mantendo-os sob a sua proteção física quando transportados para zona com menor proteção física[ix].
4. O transporte dos instrumentos de trabalho ou informação institucional para zonas menos seguras[x] deve ser antecedida da necessária autorização e da aplicação de medidas de proteção adequadas[xi].
5. Sempre que para tal sejam identificados e de forma a assegurar a atualização dos registos, os utilizadores são responsáveis por colaborar na criação e atualização de inventários dos instrumentos de trabalho e informação institucional.
6. Os utilizadores devem atuar de forma a salvaguardar o bom estado de conservação e a integridade física dos instrumentos de trabalho colocados ao seu dispor.

[vii] Através de outras informações disponíveis sobre a pessoa que define a senha, por utilização de valores por omissão, etc.

[viii] Exemplo entre ambientes diferentes, entre sistemas *core business* e sistemas de suporte, entre repositórios que contêm informação restrita e repositórios que contêm informação confidencial.

[ix] Ex. fora das instalações da SIBS.

[x] Ex. em equipamentos portáteis, em suportes amovíveis, em papel.

[xi] Por exemplo, o transporte de um suporte amovível contendo informação institucional confidencial para fora das instalações físicas da SIBS ou de um CPD/CPC para uma zona de escritórios, deve ser protegida através da cifra da informação aí contida.

7. Aquando do término/mudança de funções, os utilizadores devem devolver ao Grupo SIBS os equipamentos, suportes informativos e outros instrumentos de trabalho colocados à sua disposição para exercício dessas funções.
8. O Grupo SIBS reserva-se ao direito de eliminar dos seus sistemas qualquer material que considere ilegal ou ofensivo.
9. O Grupo SIBS poderá controlar o acesso à informação e aos dispositivos onde está armazenada, manipulada e transmitida, de acordo com a legislação nacional e as normas internas.

2.5 *Email* e *Internet*

1. Podem ser disponibilizados acessos ao sistema interno de *email* ou ligações à *Internet* para fins ligados à prossecução dos objetivos de negócio do Grupo. A utilização pessoal destes recursos é aceite, desde que não haja contradição com a boa conduta profissional e sejam respeitadas as normas de segurança.
2. Os utilizadores devem validar a exatidão, integridade, veracidade e atualidade dos dados obtidos na *Internet*. Por omissão toda a informação aí obtida deve ser tratada como suspeita[xii].
3. Os utilizadores não devem aceder a recursos da *Internet*, nem interagir/reencaminhar *emails* que lhe pareçam duvidosos, uma vez que estes poderão comprometer a segurança da informação do Grupo. Em caso de dúvida consultar previamente a AF Apoio Utilizador IT ou a AF Segurança.
4. Os utilizadores devem respeitar sempre os direitos legais (como proteção de cópia, de propriedade intelectual, etc.) associados ao *software* ou outras obras disponíveis na *Internet*. Por omissão assume-se que todos os materiais ou obras existentes na *Internet* têm direitos protegidos.
5. Os utilizadores não devem aceder à *Internet*, nem utilizar o sistema de *email* para:
    - Promover fins comerciais alheios à atividade profissional;
    - Participar em atividades, como por exemplo, *download* de ficheiros, expressar opiniões ou publicar conteúdos em *sites*, sistemas de difusão de mensagens ou fóruns que:
        - infrinjam a Lei, os direitos de autor ou outros direitos da propriedade;
        - prejudiquem a imagem do Grupo SIBS;
        - sejam ofensivas ou propositadamente geradoras de conflitos[xiii];
        - sejam obscenas;

[xii] Muita da informação nesta rede está desatualizada ou errada. Há inúmero *software* malicioso e na generalidade não é possível validar a identidade dos interlocutores. É por isso extremamente importante obter sempre confirmação da validade dos elementos obtidos na *Internet* (por exemplo, contra validando-os junto de uma fonte fidedigna).

[xiii] Nestas incluem-se todas as atividades que incluam ofensas de carácter racial, xenófobo, sexual, afirmações difamatórias ou outros comentários que visem denegrir ou ofender a dignidade, crenças religiosas ou políticas, nacionalidade ou a capacidade física ou mental de outrem.

        - patrocinem ou fomentem ações de natureza política, ideológica ou religiosa;
    - Comprometer a segurança da informação institucional ou dos sistemas e redes do Grupo SIBS;
    - Aceder de forma não autorizada ou de alguma forma comprometer ou tentar comprometer a segurança de sistemas ou redes de terceiros;
    - Aceder a *software* não autorizado com o propósito de o instalar ou utilizar nos sistemas internos;
    - Apresentar-se perante outros com uma identidade que não a sua;
    - Transmitir ou difundir informação institucional:
        - cuja divulgação não tenha sido prévia e superiormente autorizada;
        - a interlocutores não autorizados ou não corretamente identificados; ou
        - por método que não tenha sido previamente sancionado. Inclui-se neste ponto, por exemplo, o reencaminhamento dos *emails* internos para caixas de correio externas.

6. Com o objetivo de assegurar o regular funcionamento e a segurança dos sistemas e informação são utilizados meios informáticos e humanos para monitorizar e auditar, de forma aleatória e não individualizada, a utilização dos sistemas de acesso à *Internet* e *email*, podendo ainda ser auditados *emails* com visualização dos endereços, assunto e data/hora. Dada a potencial utilização pessoal destes recursos é assegurado pelo Grupo SIBS:
    - o dever de confidencialidade na monitorização/auditoria realizada;
    - que o eventual acesso a outros conteúdos só é realizado após informação/autorização do utilizador.
7. Na sua infraestrutura, a SIBS reserva o direito de impedir o acesso de/para os endereços de *email*/sistemas/serviços na *Internet* com potencial negativo na segurança dos seus sistemas/informação.

2.6 *Software* malicioso

A colaboração de cada um é essencial para evitar a exposição, execução e propagação de *software* malicioso, para tal devem ser observadas as seguintes regras:

1. Não desativar o *software anti-malware* existente nos sistemas (ex. antivírus, *host IDS*);
2. Não executar nos sistemas internos aplicações que não tenham sido aprovadas, licenciadas e sujeitas a verificação de integridade[xiv].
3. Não abrir *emails*, clicar em *links*, abrir ficheiros[xv] ou aceder a *sites* de fontes desconhecidas.

[xiv] Ex. por validação do certificado do fabricante ou por validação do *fingerprint*.

[xv] Executáveis ou de outros tipos como, por exemplo, PDF.

4. Não utilizar ou ligar aos sistemas internos, suportes, dispositivos de armazenamento ou outros que possam conter *software* malicioso. Em caso de suspeita deve ser solicitada a colaboração da AF Apoio Utilizador IT ou da AF Segurança na validação prévia dos suportes/dispositivos.
5. Não ligar os sistemas a redes diferentes das especificamente identificadas para cada sistema. Deve haver especial cuidado para evitar a ligação direta ou indireta[xvi] a redes inseguras como a *Internet* ou as suportadas em tecnologias "sem fios"[xvii].
6. Reportar à AF Apoio Utilizador IT as situações de desatualização do *software anti-malware* detetado ou todas as situações suspeitas de prefigurar infeção por *software* malicioso[xviii].

2.7 Risco

1. A disponibilidade da informação e serviços associados é fulcral para o negócio do Grupo SIBS. Todas as ações com potencial impacto na disponibilidade devem ser antecedidas de análise de risco, aplicação de medidas de controlo e aprovação adequadas.
2. Para todas as atividades que impliquem risco ou para as quais haja obrigação[xix], devem ser mantidos registos de atividade que permitam a monitorização/auditoria dessas atividades. Esses registos podem ser produzidos automaticamente pelos sistemas que implementam a atividade ou, na sua falta, devem ser produzidos manualmente pelos intervenientes nessas atividades.
3. Para reduzir a oportunidade de realização de fraude / ocorrência de "erros de simpatia", todas as atividades com risco devem ser desenhadas e implementadas de forma a limitar ou impedir a existência de situações que possam conduzir a juízos ou validações pelo (ou em proveito) próprio[xx]. Os colaboradores são responsáveis por reportar as situações deste tipo que tenham conhecimento.
4. Para limitar o risco, os colaboradores devem aplicar nas atividades, sempre que necessário, os princípios de segregação (de funções, física[xxi], lógica[xxii], etc.).
5. Os colaboradores são responsáveis pela validação da completude, integridade, acuidade, funcionalidade e operacionalidade dos trabalhos executados por terceiros cuja supervisão esteja à sua responsabilidade.

[xvi] Ex. por ligação a um dispositivo que possua uma interface de rede.
[xvii] Como as que utilizam protocolos de rádio como *wi-fi*, *Bluetooth*, GPRS/UMTS/LTE.
[xviii] Ex. sistema muito lento, sistema com comportamento anómalo.
[xix] Ex. normativa, regulamentar ou legal.
[xx] Por exemplo quem insere um pedido crítico, não deverá ser quem o aprova.
[xxi] Ex. espaços, zonas, sistemas e redes.
[xxii] Ex. ambientes, acessos.

2.8 Incidentes de segurança de informação

1. Os colaboradores têm a responsabilidade de relatar todos os incidentes de segurança e todas as situações que possam[xxiii] configurar incidentes de segurança que tenham conhecimento. O relato faz-se via um dos seguintes canais:
    - Para os eventos críticos, diretamente por telefone para o responsável da AF Segurança;
    - Para os restantes eventos, via o IntraSIBS em "Suporte | Registo de Incidentes de Segurança".

    Quem, conhecendo um incidente de segurança não o relatar, corresponsabiliza-se pelas consequências desse incidente de segurança.
2. No âmbito das suas funções todos têm a responsabilidade de colaborar com:
    - A AF Segurança na identificação, despistagem, contenção e investigação de incidentes de segurança de informação;
    - Com a AF Auditoria na realização de auditorias;
    - Com as entidades externas competentes (ex. Polícias, Tribunais) nos processos em que forem solicitados. Todo o tipo de solicitações extraordinárias de entidades externas deve ser imediatamente dado a conhecer à hierarquia.
3. O Grupo SIBS apurará as responsabilidades pelos incidentes de segurança ocorridos e promoverá, quando a situação o justificar, a:
    - divulgação às autoridades competentes[xxiv];
    - aplicação de sansões adequadas em conformidade com o expresso nos Regulamentos Internos/Lei.

2.9 Outros

Para além do expresso anteriormente, os utilizadores dos Sistemas de Informação da SIBS têm um conjunto de direitos e deveres relativos à segurança da informação que criam ou manipulam.

1. São os seguintes os direitos dos utilizadores:
    - Disporem dos mecanismos adequados para garantir a confidencialidade, integridade e disponibilidade da informação institucional;
    - Disporem de recursos e formação adequados para a realização do seu trabalho.

[xxiii] Isto é, ainda que o seu impacto não tenha ainda sido comprovado.

[xxiv] Ex. a elaboração de queixa-crime na entidade competente no caso de situações que prefigurem crime.

2. Relativamente aos deveres dos utilizadores, é-lhes solicitado que:
    - Conheçam os normativos de segurança (e de outras naturezas) do Grupo SIBS e ajam no cumprimento desses normativos e da lei e cooperem no sentido de respeitar e promover as regras relativas à segurança de informação;
    - Façam um uso adequado e responsável dos recursos informáticos do Grupo SIBS;
    - Mantenham a confidencialidade da informação a que acedem/criam de acordo com o estipulado no Acordo de Confidencialidade aplicável;
    - Ajam no cumprimento da lei e dos seus deveres profissionais de modo a não comprometer ou prejudicar a atividade e o bom nome do Grupo SIBS;
    - Contatem[xxv] a AF Segurança para esclarecimentos/resolução de situações em que constatem
        - dúvidas na interpretação ou aplicação do normativo de segurança;
        - ou a não existência de recursos para assegurar o cumprimento do normativo de segurança.

Concretizando este conjunto de deveres, não é admissível que os utilizadores:

- Observem ficheiros ou qualquer outra informação que não lhe pertença sem para isso terem sido explicitamente autorizados;
- Acedam a sistemas informáticos sem permissão explícita;
- Utilizem computadores ou redes informáticas com o intuito de caluniar, difamar ou incomodar terceiros;
- Partilhem o acesso aos sistemas informáticos ou permitam acessos não autorizados;
- Utilizem acessos privilegiados para atos que não façam parte dos seus deveres profissionais;
- Tentem circundar os mecanismos de segurança;
- Tentem intercetar ou descodificar senhas ou outra informação protegida sem autorização prévia dos Órgãos de Gestão;
- Tentem deliberadamente prejudicar ou impedir o normal e bom funcionamento dos serviços ou o desempenho dos sistemas;
- Tentem criar ou propagar *exploits* ou vírus informáticos (ou outros tipos de *malware)*;
- Tentem danificar ficheiros, equipamentos, programas ou dados que são informação institucional ou pertencem a outros;
- Usem ou tentem usar métodos de acesso não autorizados;

[xxv] O contacto com a AF Segurança faz-se preferencialmente por intermédio do sistema de pedidos de suporte existentes no IntraSIBS (Suporte | Pedido de Segurança). Alternativamente, para tratamento de questões mais específicas, pode ser utilizado o contacto de um dos *helpdesks* existentes (por exemplo, acessos.logicos@sibs.pt, helpdesk.chaves@sibs.pt, swiftnet.so@sibs.pt, helpdesk.seguranca@sibs.pt).

- Usem a conta de uma outra pessoa;
- Usem recursos do Grupo SIBS com intuitos comerciais ou para campanhas políticas;
- Usem recursos do Grupo SIBS, para fins que não estão relacionados com as atividades normais da empresa ou para suportar negócios ou empreendimentos pessoais exceto aqueles que sejam explicitamente permitidos pelas regras do Grupo.