WHITE PAPER
Los diez errores más frecuentes en Sistemas de Protección de Datos de Carácter Personal y de Seguridad de la Información

Sergio Alejandro Hernando Westerheide

Consultor de Seguridad
HISPASEC SISTEMAS
shernando@hispasec.com

Resumen

Este documento surge a raíz de algunas peticiones de información recibidas a través de nuestro servicio de atención al cliente[1]. En él pretendemos resumir parte de la experiencia profesional de Hispasec Sistemas a la hora de desplegar servicios de consultoría relativos al diseño e implementación de sistemas de gestión de la seguridad, así como servicios de adecuación técnico-legal, que en numerosas ocasiones son parte de los primeros.

El objetivo de este artículo es dar a conocer los errores más frecuentes a la hora de materializar estos sistemas. Estos fallos comunes están basados en casos que Hispasec Sistemas[2] ha encontrado en empresas reales, cuyos nombres reservamos por cuestiones de privacidad, durante la prestación de nuestros servicios a profesionales y empresas[3]. Se persigue, por tanto, que las organizaciones que estén inmersas en este tipo de despliegues o decididas a gestionar estos aspectos de la seguridad, puedan conocer qué errores son más frecuentes, y cómo solucionar dichos errores de una manera eficiente y cómoda. Con este planteamiento, la finalidad pretendida es que las no conformidades detectadas no supongan un obstáculo a la hora de completar con éxito la implantación de algún sistema de gestión que tenga que ver con la seguridad de la información.

1. Los cinco errores más frecuentes en Sistemas de Protección de Datos de Carácter Personal

Los Sistemas de Protección de Datos de Carácter Personal (SPD) tienen como misión proporcionar a las empresas e instituciones que realicen tratamiento de datos personales los mecanismos regulatorios apropiados que aseguren en todo momento que no se vulnera ninguno de los derechos de los afectados, ni ninguna otra consideración legal estipulada en los textos legales vigentes. Estos derechos implican, en esencia, la necesidad de confidencialidad, privacidad y la calidad, entendida ésta última como el acto de hacer un uso razonable de los datos, que deben ser además, adecuados, pertinentes y no excesivos.

Las referencias a errores en este tipo de sistemas se basan principalmente en la legislación española[4], ya que es España donde se han concentrado la mayoría de los despliegues de SPD realizados por Hispasec Sistemas. Muy probablemente, las medidas legales que proporciona la legislación española en la actualidad son de las más completas y estrictas en todo el ámbito mundial. En este contexto, las normas básicas a tener en cuenta son principalmente dos: la Ley Orgánica 15/1999 de 13 de Diciembre de Protección de Datos de Carácter Personal y el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal. No obstante, es muy recomendable hacer lectura de todo el canal de documentación de la Agencia Española de Protección de Datos[5] que incluye legislación relativa a todos los entornos posibles que pueden afectarnos: Legislación internacional, Unión Europea, Consejo de Europa, Iberoamérica, organismos internacionales, acuerdos de asociación de la Unión Europea, Leyes nacionales de otros países, así como la totalidad de la normativa española conexa, que es bastante amplia.

1.1. El desconocimiento de los textos regulatorios de obligado cumplimiento

Problema: El escenario principal que solemos encontrar es aquel en el que las organizaciones designan a algún empleado para que realice las labores de conformidad, como parte adicional de sus cometidos. Esto suele derivar en que el responsable designado, habitualmente desbordado por sus tareas, no puede dedicar al sistema el tiempo necesario. A consecuencia de esto, en muchos casos será imposible la conformidad no sólo por cuestiones de horario, sino de conocimientos. Esto suele provocar no sólo el descontento del responsable y el decremento de su rendimiento, al estar centrado en más cosas de las que debiera, sino que conduce habitualmente a conformidades parciales, incompletas o incluso al abandono del intento de conformidad ante la insuficiencia de conocimiento.

Solución: Las empresas que no tengan recursos humanos capaces de lograr la conformidad, en dedicación exclusiva a la misma, deberían recurrir a servicios externos. En cierto casos, si así lo aconsejase la dimensión del problema, podría recurrirse a la contratación de un experto para su incorporación en plantilla. Esto requiere

[1] sac@hispasec.com
[2] http://www.hispasec.com
[3] http://www.hispasec.com/corporate
[4] https://www.agpd.es/index.php?idSeccion=77
[5] https://www.agpd.es/index.php?idSeccion=72

que exista un CLO[6], máximo responsable de cuestiones legales en la organización que asuma el rol de la coordinación con la gerencia. Lo más saludable ante la incapacidad es la contratación de algún servicio externo, vía *outsourcing*[7].

1.2. Abandono progresivo del compromiso de la alta dirección

Problema: Pese a que en la gran mayoría de los casos las gerencias toman inicialmente el pulso en los despliegues, delegando correctamente las funciones en las personas adecuadas, se percibe que en muchas ocasiones, se abandona la supervisión de los sistemas de una manera temprana. Es muy frecuente ver cómo las gerencias negocian todos los términos de contratación, los tiempos de ejecución y las condiciones de la misma. Se prepara a la organización debidamente, pero finalmente, es habitual ver cómo ese compromiso inicial decae en el tiempo, lo que hace que disminuya el éxito de las implementaciones.

Solución: La mejor práctica para evitar este problema es que la persona designada para ejercer labores de Responsable de Seguridad[8], a la que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables, informe directamente a la gerencia, siempre y cuando la dirección haya designado algún miembro como responsable último de la organización. Estos informes deben ser semanales durante el despliegue, y al menos trimestrales durante el mantenimiento del sistema, siendo siempre aconsejable estudiar la dimensión de la implementación en cada caso.

1.3. Medidas de seguridad no aplicadas

Problema: Aunque se realice correctamente el grueso de la conformidad (elaboración del documento de seguridad, sus anexos contractuales y la comunicación de ficheros), es habitual comprobar como no se llevan a cabo tareas posteriores. Un ejemplo puede ser la implantación de las medidas a las que obliga el Real Decreto 994/1999, habitualmente denominado Reglamento de Seguridad.

Solución: Una vez que el Responsable de Seguridad conoce todo el alcance del sistema y recibe las instrucciones adecuadas, debe incluír un capítulo en sus informes a gerencia dedicado exclusivamente al nivel de cumplimiento de las medidas de seguridad aplicables en cada caso. Las medidas del Reglamento de Seguridad significan la materialización de los requisitos legales de la Ley Orgánica, y por tanto, son de obligatorio y necesario cumplimiento.

1.4. Ausencia de mantenimiento

Problema: Es habitual encontrar organizaciones que contratan la conformidad, pero que abandonan cualquier práctica de mantenimiento una vez han finalizado los servicios de consultoría externa. A consecuencia de esto, cuando se plantean las revisiones trimestrales, los informes a gerencia y las auditorías obligatorias en los supuestos que la Ley prevé[9], los sistemas se encuentran obsoletos, carentes de sentido y totalmente ajenos a la realidad. Además de ser poco útiles, serán insuficientes para cumplir con la legislación, que contempla expresamente el capítulo de mantenimiento como necesario.

Solución: Se debe forzar un período de mantenimiento de todo el sistema. Al menos trimestralmente, mediante los controles trimestrales de verificación, y siempre que se produzca algún cambio significativo en el sistema. En estos casos, el Responsable de Seguridad debe anotar todos los cambios que precisen ser reflejados en la documentación, y debe comunicar a gerencia dichos cambios, para que la dirección los apruebe. Es aconsejable que exista una cadena de elaboración, revisión y aprobación que no deje lugar a dudas en cuanto a la responsabilidad de quién elabora los cambios, quién los revisa y quién los aprueba, de modo que la trazabilidad de responsabilidad sea auditable.

1.5. Aislamiento del sistema

Problema: Es frecuente que las organizaciones no se planteen la posibilidad de integrar estos sistemas en los ya existentes, dejándolos en el más profundo aislamiento. Es perfectamente posible, y de hecho recomendable, integrar los sistemas de gestión en la empresa, y los sistemas de adecuación legal no son una excepción. A veces es tan sencillo como, por ejemplo, integrarlos en sistemas ISO 9001:2000 de gestión de la calidad[10], estableciendo en el capítulo de requisitos reglamentarios y legales la conformidad, o exigiendo a los proveedores el cumplimiento de las normativas como un requisito para proveer a la organización. En el caso de SGSI, es más sencillo, ya que existe un dominio de control específicamente dedicado a la conformidad legal, concretamente en el punto 15.1 de ISO 17799:2005[11], en el que se declaran los requisitos de conformidad legal.

Solución: Integrar los sistemas todo lo posible, de forma que compartan recursos aprovechables en cada uno de los sistemas. El responsable de seguridad debe mantener reuniones periódicas para conocer los avances en otros sistemas de gestión de la empresa, de modo que estos comités sirvan para promover medidas de integración a todos los niveles.

2. Los cinco errores más frecuentes en Sistemas de Gestión de Seguridad de la Información

Los Sistemas de Gestión de Seguridad de la Información (SGSI) son los que tienden a integrar en las organizaciones la seguridad como un proceso más entre los existentes en un mapa de procesos, tanto en su concepción, definición, mecanismos de medición y de corrección ante desviaciones. Los procesos de seguridad tienden a afectar a todos los procesos de la organización, con lo que los SGSI[12] suelen ser sistemas donde se coloca en el centro de la organización todo lo inherente a las tecnologías de la información, al igual que un sistema de Gestión de la Calidad ISO 9001:2000 tiende a colocar a los clientes en

[6] Chief Legal Officer

[7] Externalización, acto de contratación de servicios a un tercero especialista

[8] Artículo 2 del Real Decreto 994/1999

[9] Artículo 17 del Real Decreto 994/1999

[10] http://es.wikipedia.org/wiki/Sistema_de_gestin_de_la_calidad

[11] http://en.wikipedia.org/wiki/ISO/IEC_17799

[12] http://en.wikipedia.org/wiki/Information_security

el centro de los objetivos organizacionales.

Es habitual que este tipo de sistemas se soporte en especificaciones internacionales, siendo las adaptaciones hechas en los países posibles, si bien, como es obvio, lo más recomendable es alinearse con los estratos superiores, por una cuestión de trazabilidad. A tal efecto los principales marcos normativos son, actualmente, ISO 17799:2005 e ISO 27001:2005[13]

2.1. Política de seguridad incorrecta

Problema: En numerosas ocasiones, la política de seguridad del SGSI, de la que emana el resto del sistema, es incorrecta, bien por exceso, bien por defecto. Es frecuente observar aquí también una diseminación incorrecta de la política, la cual debe estar siempre patrocinada por la gerencia para garantizar su máxima difusión, conocimiento y cumplimiento.

Solución: La política de seguridad no debe ser menoscabada por el hecho de que sea una visión general del sistema y no proporciones materialización concreta sobre la seguridad. Debe ser lo suficientemente genérica para no tener que cambiarla constantemente, y debe ser lo suficientemente acotada para que represente los objetivos en materia de seguridad la máxima concreción. Debe estar impulsada siempre por la gerencia, la cual tiene la responsabilidad directa de su correcta diseminación.

2.2. Gestión del riesgo inadecuada

Problema: Se observa con demasiada frecuencia que la gestión del riesgo no es adecuada, generalmente no por exceso sino por defecto. Esto suele tener implicaciones muy serias en la continuidad del negocio y los sistemas de recuperación[14], que se diseñan y dimensionan a partir de un mapa de riesgos que debe ser lo más acertado posible.

Solución: La gestión del riesgo[15] debe ser milimétricamente estudiada. Es, con toda probabilidad, el campo que menor tolerancia a la indeterminación y a la inconcreción admite, ya que el mapa de riesgos tiene implicaciones directas en todo el sistema, con lo que las desviaciones cometidas en la elaboración del mismo suelen acarrear desviaciones en todas las áreas que podrían hacer inútil el sistema.

2.3. Gestión de la continuidad insuficiente

Problema: Con relativa frecuencia es posible comprobar que la gestión de la continuidad[16], parte esencial dentro de los SGSI, no termina de ser todo lo adecuada que debiera. El problema de esta gestión insuficiente es doble, ya que la gestión de la continuidad va de la mano de la recuperación ante incidentes. Es lo que habitualmente se conoce como BC/DR.[17]

Solución: La gestión de la continuidad debe ser un elemento con prioridad absoluta dentro del SGSI. Debe ser igualmente proporcional, y debe basarse en los resultados de las mediciones de riesgo efectuadas en el análisis de los mismos, con lo que la gestión BC/DR[18] pasa siempre por una revisión de la gestión del riesgo, y de una planificación adecuada ante la probabilidad de ocurrencia, severidad y medidas a tomar para cada uno de los riesgos identificados.

2.4. Sistemas no proporcionales a las organizaciones

Problema: Los SGSI son habitualmente voluminosos. Contamos con la gran ventaja de que los textos que definen los mismos no son de obligado cumplimiento, sino guías y buenas prácticas para poder materializar un SGSI. Esto nos deja manga ancha para poder tomar de las normas aquello que más nos convenga y en la secuencia temporal más adecuada. Si tratamos de implantar un SGSI en una organización, debemos ir hito a hito, de una manera secuencial, ya que es la única manera de poder cuantificar las desviaciones e ir puliendo defectos sobre la marcha, tal y como sugiere la filosofía de mejora continua. Es muy habitual ver como las empresas se plantean los SGSI para ser desplegados de forma global, sin progresividad, resultando los sistemas implantados en sistemas rígidos y poco orientados a los cambios constantes que requiere un SGSI.

Solución: Sea gradual. Plantee para el sistema una rueda PDCA[19], en el que pueda, para cada parcela, poder establecer un plan (*Plan*), realizar acciones (*Do*), verificar (*Check*) y por último, actuar en función a las desviaciones (*Act*). Tenga en cuenta que un SGSI puede implicar miles de horas de consultoría para los casos más extensos, con lo que ser gradual y planificado es esencial.

2.5. Organizaciones que se adaptan a los sistemas y no sistemas que se adaptan a las organizaciones

Problema: Como nota final, a modo de resumen, es frecuente observar que algunos SGSI se aplican sin que exista personalización. Un SGSI es un traje del que, por desgracia, nunca hallaremos nuestra talla en ningunos grandes almacenes ni en ninguna tienda de ropa. Hay que recurrir siempre a un sastre que ajuste el sistema a todos los requisitos de la organización. Tal y como sucede con la ropa, adquirir un traje que nos venga algo grande o algo pequeño para salir del paso es una solución que no redunda en beneficio a largo plazo, y que puede provocar problemas serios en la continuidad. Los SGSI no pueden suministrarse ni implementarse como servicios generalistas.

Solución: Entienda a los SGSI no como un coste, sino como una inversión. Confíe en el retorno de la inversión[20] que producen siempre los sistemas correctamente desplegados.

3. Conclusiones

Las principales conclusiones a las que podemos llegar, en lo relativo a errores más frecuentes en cualquier sistema de gestión, son principalmente las siguientes:

[13] Ambas normas pueden ser adquiridas en el comercio online de ISO, ubicado en `http://www.iso.org`

[14] `http://www.hispasec.com/unaaldia/2740`

[15] `http://www.csi.map.es/csi/pg5m20.htm`

[16] `http://en.wikipedia.org/wiki/Business_continuity_planning`

[17] Business Continuity / Disaster Recovery

[18] `http://www.hispasec.com/unaaldia/2740`

[19] `http://es.wikipedia.org/wiki/PDCA`

[20] `http://www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf`

1. Los sistemas tienen que estar promovidos y estimulados por la alta dirección.
2. Pese a que la alta dirección debe estar plenamente involucrada en la diseminación y en los aspectos más estratégicos del sistema de gestión, debe delegarse correctamente en los escalafones inferiores para que los planes a largo plazo inherentes al sistema se traduzcan en acciones operativas, en el medio y el corto plazo.
3. Los sistemas de gestión sólo son poderosos y útiles cuando se diseñan, se despliegan y se mantienen con corrección y solvencia. Externalice si no puede atender cualquiera de esas tres fases.
4. Sea gradual a la hora de implantar un sistema de cualquier tipo. A mayor extensión de los sistemas, se requiere siempre una planificación más escalonada.
5. Jamás entienda a la certificación como la única razón de ser a la hora de desplegar un sistema. La certificación sólo es un premio opcional para los sistemas correctamente desplegados.

4. Referencias

[1] *Hispasec Sistemas. Servicios de seguridad para empresas, instituciones y profesionales.* http://www.hispasec.com/corporate

[2] *10 claves para una adecuada recuperación ante desastres.* http://www.hispasec.com/unaaldia/2740

[3] *La recuperación de datos, un arma de doble filo.* http://www.hispasec.com/unaaldia/2715

[4] *Seguridad informática y protección de datos.* http://www.hispasec.com/unaaldia/2515

[5] *Pequeños dispositivos, grandes problemas.* http://www.hispasec.com/unaaldia/2757

[6] *El enemigo puede estar dentro.* http://www.hispasec.com/unaaldia/2448

[7] *Planes de recuperación ante desastres.* http://www.hispasec.com/unaaldia/2540

[8] *La seguridad corporativa continúa infrapresupuestada.* http://www.hispasec.com/corporate/noticias/27

[9] Peltier, Thomas R. "Information Security Policies, Procedures and Standards: A Practitioner's Reference, Second Edition". CRC Press, 2004. ISBN: 0849319587

[10] Desman, Mark D. "Building an Information Security Awareness Program". CRC Press, 2002. ISBN: 0849301165

[11] Purser, Steve " A Practical Guide to Managing Information Security". Artech House Publishers, 2004. ISBN: 1580537022

[12] Maiwald, Erik "Security planning and disaster recovery". Mc Graw Hill, 2002. ISBN: 0072224630

[13] Camp, L. Jean "Economics of Information Security". Springer, 2004. ISBN: 140208089

[14] Wallace, Michael "The disaster recovery handbook". American Management Association, 2004. ISBN: 0814472400

5. Licencia

[21] `http://creativecommons.org/licenses/by-nc-sa/2.5/es/`