Actividad 3: Análisis y gestión de riesgos

Seguridad Informática

Orquidea Seijas
GRADO EN INGENIERÍA INFORMÁTICA Escola Técnica Superior de Ingeniería

CONTENIDO

1. Herramienta pilar 2
   I. Comprobación de los campos que aparecen en la descripción del proyecto 2
   II. Análisis de riesgos 3
      i. Ejemplos de activos 3
      ii. Ejemplos de dependencias de activos 3
      iii. Ejemplos de las amenazas que se consideran de mayor impacto 3
   III. Exploración de las salvaguardas 5
      i. [COM] Protección de las comunicaciones 5
      ii. [IA] Identificación y autenticación 5
      iii. [PPS] Protección del perímetro físico 5
      iv. [D] Protección de la información 5
      v. [K] Gestión de claves criptográficas 6
   IV. Impacto y Riesgo 6
      i. Impacto potencial más elevado 6
      ii. Impacto potencial menos relevante 6
      iii. Diferencia entre las fases Potencial, Actual y Objetivo. 7
   V. Perfiles de seguridad 7
      i. Normas ISO/IEC 27002 7
      ii. Reglamento LOPD 7
2. Herramientas de autoevaluación de la normativa ISO/IEC 27001, 27002 9
   I. Descripción de la empresa 9
   II. Cuestionario ISO/IEC 27001. Norma certificable 10
   III. Cuestionario ISO/IEC 27002. Buenas prácticas de seguridad 11
   IV. Mejoras propuestas a partir de los resultados de las auditorías 12

Referencias 13

1. HERRAMIENTA PILAR

I. COMPROBACIÓN DE LOS CAMPOS QUE APARECEN EN LA DESCRIPCIÓN DEL PROYECTO

En primer lugar, se ha abierto la herramienta PILAR y se ha seleccionado el modo Presentación. Se ha ejecutado el programa con la configuración de Análisis y Gestión de Riesgos, en modo cualitativo, y se ha abierto el fichero de ejemplo. A partir del subconjunto de dimensiones, se indicarán las dimensiones de seguridad contempladas en el proyecto. Estas son:

- **[D] disponibilidad:** propiedad o característica de los activos consistente en que las entidades o procesos autorizado tienen acceso a los mismos cuando lo requieren.
- **[I] integridad de los datos:** propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- **[C] confidencialidad de los datos:** propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- **[A] autenticidad de los usuarios y de la información:** propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- **[T] trazabilidad del servicio y de los datos:** propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

El subconjunto de criterios de valoración es el siguiente que se ha propuesto analizar. Se han seleccionado tres criterios considerados para la valoración de activos a modo de ejemplos. A su vez, se han seleccionado dentro de los tres criterios, los dos riesgos más graves y los dos más leves.

En primer lugar, se ha seleccionado el criterio de *Información Personal*, que es un activo que se verá afectado de diferentes formas si se cumple un riesgo y esta información se ve comprometida:

- Probablemente afecte gravemente a un grupo de individuos.
- Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.
- Pudiera causar molestias a un individuo.
- Pudiera quebrantar de forma leve leyes o regulaciones.

En segundo lugar, se ha seleccionado el criterio de *Obligaciones legales*:

- Probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación.
- Probablemente cause un incumplimiento grave de una ley o regulación.
- Probablemente sea causa de un incumplimiento de una ley o regulación.
- Pudiera causar el incumplimiento leve o técnico de una ley o regulación.

Finalmente, se ha seleccionado el criterio de *Seguridad de las personas*:

- Podría causar la pérdida de muchas vidas humanas.
- Podría causar la pérdida de una o más vidas humanas.
- Podría lesionar levente a un individuo.
- Podría lesionar levemente a un individuo.

En general, se puede inferir que los criterios de valoración seleccionados están relacionados con posibles amenazas a vidas humanas, posibles problemas legales y posibles molestias para los usuarios.

II. ANÁLISIS DE RIESGOS

A continuación, se explorarán los apartados de activos, dependencias entre activos y amenazas. Antes de explorarlos, es necesario repasar el concepto de activo y el de amenaza. Por un lado, un activo es un elemento con algún valor para la organización, tal y como se explicó en clase de teoría, y que debe protegerse. Por otro lado, una amenaza es un evento que tiene el potencial de dañar a un activo.

i. Ejemplos de activos

- **[B] Información y servicios:** [INFO] expedientes en curso, [S_in_person] tramitación personal y [S_remote] tramitación remota.
- **[IS] Servicios internos:** [https] acceso SSL de los usuarios, [email] mensajería electrónica, [archive] archivo histórico central, etc.
- **[E] Equipamiento:** [SW] aplicaciones ([SW_app] tramitación de expedientes), [HW] equipos ([PC] puestos de trabajo, [SRV] servidor), [COM] comunicaciones ([LAN] red local, [firewall] cortafuegos), etc.
- **[SS] Servicios subcontratados:** [ADSL] conexión a Internet.
- **[L] Instalaciones:** [offices] oficinas y [dc] salas de equipos.
- **[P] Personal**

ii. Ejemplos de dependencias de activos

- **[PC] Puestos de trabajo:** depende de [offices] Oficinas.
- **[ADSL] Conexión a Internet:** depende de [dc] salas de equipos.
- **[firewall] Cortafuegos:** depende de [dc] salas de equipos.
- **[LAN] Red local:** depende de [offices] Oficinas y de [dc] salas de equipos.
- **[email] Mensajería electrónica:** depende de [S_Internet] Acceso a Internet.

iii. Ejemplos de las amenazas que se consideran de mayor impacto

- [N.*] Desastres naturales.
- [I.1] Fuego.
- [I.9] Interrupción de otros servicios o suministros esenciales.
- [E.24] Caída del sistema por agotamiento de recursos.
- [A.18] Destrucción de la información.
- [A.26] Ataque destructivo.

Como objetivo de la práctica, se ha solicitado la búsqueda de ejemplos de activos que se vean afectados por los errores de usuario y activos que se vean afectados por el fuego. En el primer caso, los activos afectados son:

- [S_in_person] Tramitación presencial.
- [S_remote] Tramitación remota.
- [email] Mensajería electrónica.
- [archive] Archivo histórico central.
- [PC] Puestos de trabajo.
- [SRV] Servidor

En el segundo caso, los activos afectados por el fuego son:

- [PC] Puestos de trabajo.
- [SRV] Servidor.
- [LAN] Red Local.
- [offices] Oficinas.
- [dc] Sala de equipos.

También se ha solicitado la búsqueda de ejemplos de amenazas que afecten a los datos de los usuarios y amenazas que afecten al procesado de los datos. Para el primer caso, se han seleccionado activos a los que están asociados los datos de usuarios ([https] acceso SSL de los usuarios, [email] Mensajería electrónica y [archive] Archivo histórico central) para la obtención de las amenazas asociadas. Una vez obtenidas, se han seleccionado las que podrían afectar directamente a los datos de usuarios:

- [I.8] Fallo de servicios de comunicaciones.
- [I.9] Interrupción de otros servicios o suministros esenciales.
- [E.1] Errores de los usuarios.
- [E.2] Errores del administrador del sistema / de la seguridad.
- [E.15] Alteración de la información.
- [E.18] Destrucción de la información.
- [E.19] Fugas de información.
- [A.6] Abuso de privilegios de acceso.
- [A.7] Uso no previsto.
- [A.11] Acceso no autorizado.
- [A.12] Análisis de tráfico.
- [A.15] Modificación de la información
- [A.18] Destrucción de la información.
- [A.19] Revelación de información.

Para el segundo caso se han seleccionado activos a los que está asociado el procesado de datos([INFO] Expedientes en curso, [S_in_person] Tramitación personal y [S_remote] Tramitación remota) para la obtención de las amenazas asociadas:

- [E.1] Errores de los usuarios.
- [E.2] Errores del administrador del sistema / de la seguridad.
- [E.15] Alteración de la información.
- [E.18] Destrucción de la información.
- [E.19] Fugas de información.
- [E.24] Caída del sistema por agotamiento de recursos.
- [A.5] Suplantación de la identidad.
- [A.6] Abuso de privilegios de acceso.
- [A.7] Uso no previsto.
- [A.11] Acceso no autorizado.
- [A.13] Repudio (negación de actuaciones).
- [A.15] Modificación de la información.
- [A.18] Destrucción de la información.
- [A.19] Revelación de información.
- [A.24] Denegación de servicio.

III. EXPLORACIÓN DE LAS SALVAGUARDAS

A continuación, se realizará una exploración de las salvaguardas, concretamente de los siguientes tipos: para la protección de las comunicaciones, para la identificación y autenticación, para la protección del perímetro físico, para la protección de la información y para la gestión de claves criptográficas.

Se seleccionarán ejemplos asociados a los tipos mencionados previamente, con el nivel de recomendación más alto de las salvaguardas. Estas son salvaguardas para las que tiene un mayor interés su aplicación.

i. [COM] Protección de las comunicaciones

- [COM.SC] Se aplican perfiles de seguridad. (Nivel de recomendación: 8/10).
- [COM.SC.3] Se eliminan, o modifican, las cuentas estándar de usuario. (Nivel de recomendación: 8/10).
- [COM.SC.4] Sólo los administradores de seguridad autorizados pueden modificar la configuración. (Nivel de recomendación: 8/10).
- [COM.SC.5] Los servicios activados se configuran de forma segura. (Nivel de recomendación: 8/10).
- [COM.wifi] Seguridad *Wireless.* (Nivel de recomendación: 7/10).

ii. [IA] Identificación y autenticación

- [IA.7] {xor} Factores de autentificación que se requieren. (Nivel de recomendación: 8/10).
- [IA.7.3] Certificados software (criptografía de clave pública). (Nivel de recomendación: 8/10).
- [IA.7.4] Algo que se es – biometría (ej. Huella dactilar). (Nivel de recomendación: 8/10).
- [IA.7.4.2] El mecanismo se inhabilita cuando se ve comprometido o hay sospecha de ello. (Nivel de recomendación: 8/10).
- [IA.7.9] 2 factores: biometría + contraseña. (Nivel de recomendación: 8/10).

iii. [PPS] Protección del perímetro físico

- [L.depth] Defensa en profundidad. (Nivel de recomendación: 5/10).
- [L.IA]{xor} Mecanismo de autenticación. (Nivel de recomendación: 5/10).
- [L.AC] Control de los accesos físicos. (Nivel de recomendación: 5/10).
- [PPS.g] La seguridad de la instalación no es responsabilidad de un único guarda. (Nivel de recomendación: 5/10).

iv. [D] Protección de la información

- [D.backup] Copias de seguridad (*backups*). (Nivel de recomendación: 6/10).
- [D.DS] Uso de firmas electrónicas. (Nivel de recomendación: 6/10).
- [D.I] Protección de la integridad. (Nivel de recomendación: 5/10).
- [D.4] Protección de la confidencialidad. (Nivel de recomendación: 5/10).
- [D.TS] Uso de servicios de fechado electrónico (*time stamping*). (Nivel de recomendación: 5/10).

v. [K] Gestión de claves criptográficas

- [K.comms] Protección de claves de comunicaciones. (Nivel de recomendación: 8/10).
- [K.comms.5] Las claves se generan en un entorno separado del de explotación.(Nivel de recomendación: 8/10).
- [K.comms.7] {xor} Distribución de claves (Nivel de recomendación: 8/10).
- [K.comms.7.1] Contenedor seguro (Nivel de recomendación: 8/10).
- [K.comms.8]{xor} Almacenamiento de las claves (Nivel de recomendación: 7/10).

IV. IMPACTO Y RIESGO

En este apartado, se accederá a la ventana de impacto y riesgo con el fin de buscar ejemplos de impacto potencial más elevado y de impacto potencial menos relevante. También se indicará a qué activo y a qué dimensión afectan.

i. Impacto potencial más elevado

Para el activo *[S_in_person] Tramitación presencial*, se han encontrado varias amenazas que, de cumplirse, tendrían un impacto potencial elevado:

- **[A.5] Suplantación de la identidad:** afecta a la dimensión [A] autenticidad de los usuarios y de la información y es de nivel de impacto [7]. También afecta a la dimensión [C] confidencialidad de los datos, pero con un nivel de impacto un poco más bajo: [6].
- **[A.11] Acceso no autorizado:** afecta a la dimensión [A] autenticidad de los usuarios y de la información y es de nivel [7]. También afecta a la dimensión [C] confidencialidad de los datos, pero con un nivel de impacto un poco más bajo: [6].

Para el activo [PC] Puestos de trabajo, también se han encontrado amenazas que podrían tener un impacto potencial elevado:

- **[A.22] Manipulación de programas:** en este caso se afecta a las dimensiones [C] confidencialidad de los datos e [I] integridad de los datos por igual, con un impacto de nivel [7].
- **[A.11] Acceso no autorizado:** en este caso, afecta a la dimensión [D] disponibilidad con un impacto de nivel [7].

Finalmente, para el activo [ADLS] Conexión a Internet, se ha seleccionado una amenaza con impacto de nivel [7] asociada a T] trazabilidad del servicio y de los datos. Esta amenaza es:

- **[A.13] Repudio (negación de las actuaciones).**

ii. Impacto potencial menos relevante

Para el activo *[S_in_person] Tramitación presencial*, se ha encontrado una amenaza que, de cumplirse, tendría un impacto potencial poco relevante en una única dimensión (las demás no se verían afectadas):

- **[A.6] Alteración de la información:** en este caso, afecta a la dimensión [I] integridad de los datos con un impacto de nivel [0].

Para el activo *[SW_app] Tramitación de expedientes*, se ha encontrado una amenaza que, de cumplirse, tendría un impacto potencial poco relevante en dos dimensiones (las demás no se verían afectadas):

- **[E.21]Errores de mantenimiento / actualización de programas (software):** en este caso, afecta a la dimensión [I] integridad de los datos y a la dimensión [D] disponibilidad con un impacto de nivel [0].

Para el activo *[PC] Puestos de trabajo*, se ha encontrado varias amenazas que, de cumplirse, tendrían un impacto potencial poco relevante en una dimensión (las demás no se verían afectadas):

- **[N.2] Daños por agua:** en este caso afecta a la dimensión [D] disponibilidad con un impacto de nivel [0]
- **[I.4] Contaminación medioambiental:** en este caso afecta a la dimensión [D] disponibilidad con un impacto de nivel [0]

iii. Diferencia entre las fases *Potencial*, *Actual* y *Objetivo*.

En primer lugar, la fase *Potencial* registra y enseña el impacto que puede tener una amenaza de no haber aplicado ningún tipo de salvaguarda sobre ella. Es por ello por lo que, en ella, hay muchos niveles de impacto al máximo.

En segundo lugar, la fase *Actual* contiene el impacto que tiene una amenaza tras la aplicación de una o varias salvaguardas. Esta fase enseñaría el impacto real de una amenaza si se produjera en ese instante.

Finalmente, la fase *Objetivo* enseña el propósito final de la empresa u organismo respecto al impacto de las amenazas, es por ello por lo que casi todos los impactos asociados a amenazas tienen un nivel de impacto [0].

V. PERFILES DE SEGURIDAD

En este apartado se observará en la herramienta PILAR los aspectos cubiertos en los informes de seguridad según las normas ISO/IEC 27002 (Buenas prácticas, versión 2013) y según el reglamento LOPD. Para cada una de estas normas se enseñarán algunos ejemplos del grado de cumplimiento de cada una de las normas. Este grado se mide en seis niveles: L0, L1, L2, L3, L4 y L5, siendo L0 un proceso inexistente, L1 un proceso inicial, L2 un proceso reproducible pero intuitivo, L3 un proceso definido, L4 un proceso gestionado y medible y L5 un proceso optimizado.

i. Normas ISO/IEC 27002

En este caso, se presentan dos opciones para el cumplimiento de la norma: el *Actual* y el *Objetivo*. Para los ejemplos seleccionados se tendrá en cuenta el cumplimiento actual.

- **L0:** [G.3.3] Normas de seguridad.
- **L1:** [SW.start.3] Se requiere autorización previa.
- **L2:** [S.CM.1] Se dispone de normativa de control de cambios.
- **L3:** [SW.CM.1] Se dispone de una política.
- **L4:** [S.2.2.1] Se define la política aplicable sobre seguridad de la información
- **L5:** [S.2.4.1] Se establece un protocolo formal para la modificación de los servicios prestados

ii. Reglamento LOPD

- **L0:** [96.1] auditoría periódica
- **L1:** [AC.2.6] {xor} Modelo de control de acceso

- **L2:** [G.3.2] Política de Seguridad de la Organización
- **L3:** [AC.2.2] Se restringe el uso de las utilidades del sistema
- **L4:** [94.4] datos para pruebas
- **L5:** [G.1.4] Asignación de responsabilidades para la seguridad de la información

2. HERRAMIENTAS DE AUTOEVALUACIÓN DE LA NORMATIVA ISO/IEC 27001, 27002

En esta parte de la práctica ha sido necesario considerar una empresa sobre la que se hará un diagnóstico respecto al grado de cumplimiento de la norma ISO/IEC 27001, asumiendo que tiene ciertas medidas de seguridad (técnicas y organizativas) ya implantadas. Para ello se cubrirán dos cuestionarios, el primero para ver el grado de cumplimiento de la norma ISO/IEC 27001, y el segundo, sobre la guía de buenas prácticas (ISO/IEC 27002).

I. DESCRIPCIÓN DE LA EMPRESA

Se ha escogido como empresa a analizar una empresa de reformas ficticia, *Empresa S.L.*. Esta empresa cuenta con alrededor de diez trabajadores, todos ellos con su propio equipo y con acceso restringido en menor o mayor medida a los datos de la empresa: clientes, proyectos, materiales en el almacén, permisos del ayuntamiento, entre otras.

Esta empresa cuenta con mantenimiento externo informático, ya que tienen una empresa subcontratada para ello. Esta empresa no solo se encarga de instalar y actualizar, sino de proteger por sus equipos, su red y su base de datos. Si bien *Empresa S. L.* no cuenta con documentación formal que refleje estándares de seguridad informática, sí que tiene procedimientos informales para la realización de tareas para el mantenimiento de la seguridad.

La encargada de realizar la auditoría sobre el cumplimiento de las normativas de seguridad es una empresa informática que ha sido recientemente contratada. La auditoría contratada es sumamente importante, por lo que necesitan realizar la operación sin tener en cuenta auditorías anteriores para no verse influenciados por resultados previos.

A los dueños de *Empresa S.L.* les fundamental saber si su empresa cumple con los estándares de seguridad ya que la Agencia Nacional de Inteligencia está buscando una empresa para realizar una reforma en su sede. Esta agencia, necesita una empresa cuya seguridad informática sea certificable para llevar a cabo la reforma.

II. CUESTIONARIO ISO/IEC 27001. NORMA CERTIFICABLE

En primer lugar, es necesario explicar qué representa la columna *Findings* en el cuestionario de auditoría. Esta columna representa lo que se "encuentra" sobre la empresa al rellenar el cuestionario, es decir: información importante que no se puede representar a través de un porcentaje. Al rellenar el cuestionario que se encuentra en el anexo "Orquídea_Seijas_iso_27001_compliance_checklist.xsl", se escribieron varios comentarios en la columna de *Findings* con el fin de incluir información aportada por la empresa en el momento de la auditoría.

Tras realizar el cuestionario, estos fueron los resultados en general:

Domain	Status (%)
Security Policy	64%
Organization of Information Security	44%
Asset Management	52%
Human resources security	50%
Physical and Enviornmental security	72%
Communication and Operations Management	64%
Access Control	76%
Information system acquisition, development and maintanence	57%
Information security incident management	74%
Business Continuity Management	67%
Compliance	66%

Ilustración 1 Resultados de cada apartado de la auditoría para ISO/IEC 27001

Tal y como se puede ver en la Ilustración 1, y como era de esperar, en general Empresa S.L. tiene posibilidades de obtener una certificación de ISO/IEC 27001. Si bien no hay ninguna puntuación por encima del 85%, que se consideraría como excelente, no hay ninguna por debajo del 25%, lo que se consideraría desastroso.

Por un lado, solo ha obtenido una puntuación menor del 50% en un punto: *Organización de la seguridad de la información*. Esto es razonable ya que, como se comentó en la presentación de la empresa, no tiene documentación formal estándar para los elementos de seguridad, pero sí tiene procedimientos informales.

Por otro lado, la mejor puntuación es la de *Manejo de incidentes relacionados con la seguridad de la información*. Esto tiene sentido, ya que, si bien no tienen ningún documento formal, se trata de una empresa con pocos trabajadores: siempre es posible contactar con el trabajador con mayor rango de autoridad y consultar sobre incidentes. Además, los incidentes directamente relacionados con la seguridad informática están controlados por la empresa externa, por lo que se puede decir que estos están correctamente asegurados.

III. CUESTIONARIO ISO/IEC 27002. BUENAS PRÁCTICAS DE SEGURIDAD

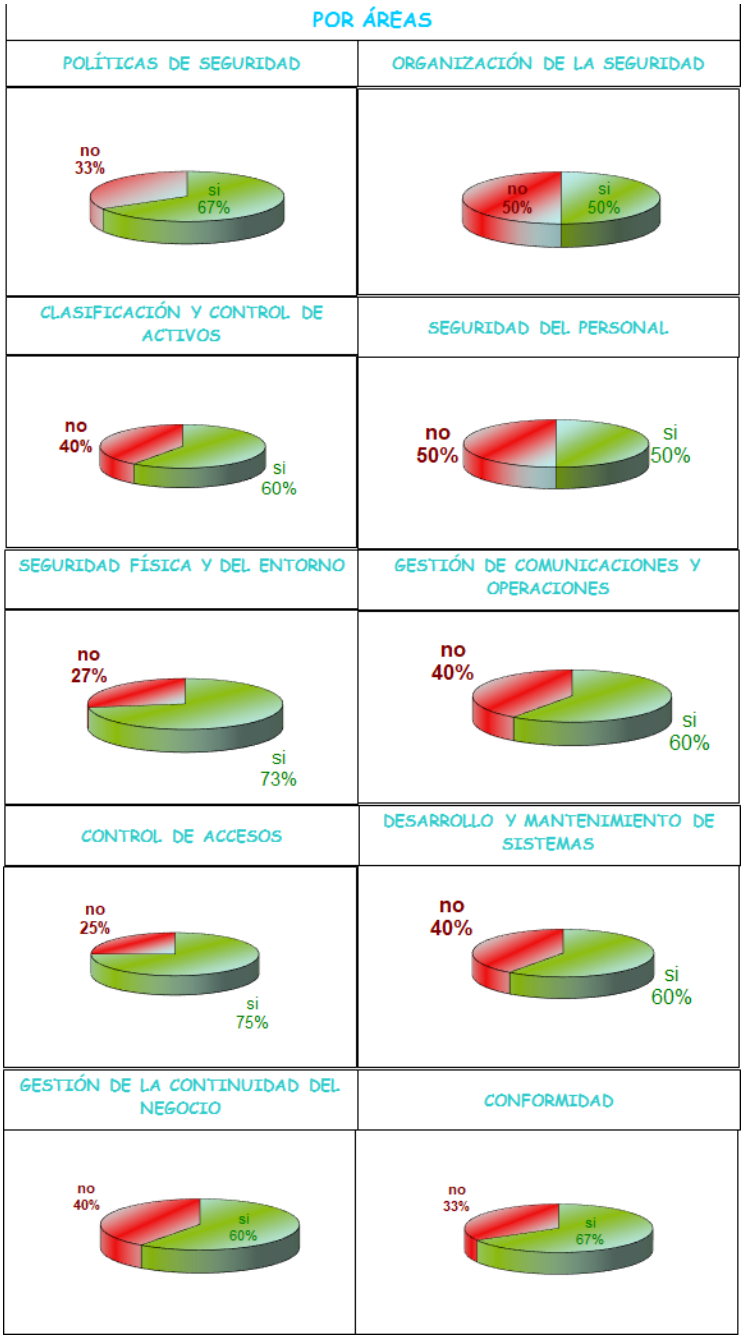

Ilustración 2Resultados de cada apartado de la auditoría para ISO/IEC 27002

En este caso, el cuestionario a realizar se trata de una autoevaluación, con menos apartado y menos técnica que la auditoría del apartado anterior. En este caso, se tratará de ver si *Empresa S.L.* realiza prácticas de seguridad correctas.

Tal y como se puede ver en la Ilustración 2, en este caso tampoco se obtiene ninguna puntuación inferior al 25% en ningún punto del cuestionario. De hecho, y a diferencia del apartado anterior, tampoco se llega a bajar del 50%. Esto sucede puesto que el número de preguntas realizadas sobre cada apartado era menor y, por lo tanto, cada pregunta era más general. No existía un punto

medio: o se realizaba la acción preguntada (aunque fuera mínimamente) o no se realizaba en absoluto, lo que pudo beneficiar a algunos puntos.

En este caso, los apartados con una puntuación más baja están empatados con 50% y son: *Organización de la seguridad* y *Seguridad del personal*. Para el primer caso, ya se comentó la justificación de la puntuación, tanto en el apartado anterior como en la presentación de la empresa. El segundo caso, sin embargo, no se ve reflejado en la auditoría realizada en el apartado anterior, ya que trata la seguridad física y del entorno en el mismo apartado. La seguridad del personal recibe esta puntuación del 50% ya que, si bien pueden acceder a la información de seguridad informalmente a través de interacción con sus superiores, no cuentan con ningún tipo de documentación formal ni de formación en seguridad de la información por parte de la empresa.

Para la autoevaluación, el apartado con mayor puntuación es, con un 75%, el *Control de Acceso*. Para poder acceder tanto a la sede física de la empresa como a la sede virtual, es necesario pasar por un proceso de identificación. Por una parte, en la sede física, se accede a través del reconocimiento por parte del encargado de seguridad. Por otra parte, para acceder a la sede virtual, no sólo desde redes externas, sino desde los propios ordenadores internos, es necesario introducir credenciales compuestas de un identificador unívoco y una contraseña alfanumérica con un mínimo de ocho caracteres.

IV. MEJORAS PROPUESTAS A PARTIR DE LOS RESULTADOS DE LAS AUDITORÍAS

Tras el análisis de las auditorías, una mejora importante para esta empresa sería, en general, actualizar y añadir documentación relacionada con la seguridad. Esto serviría para que los empleados tengan un sitio al que acceder cuanto tengan dudas sobre posibles incidentes o sobre su propia seguridad y también para que exista un registro de las políticas actuales de la empresa.

Otra mejora interesante sería fomentar la formación en seguridad informática por parte de los empleados. Esta formación ayudaría a facilitar la creación de protocolos de seguridad y también ayudaría a seguirlos. Además, así sería posible ahorrar costes en mantenimiento informático, ya que los empleados serían más cuidadosos, al ser más conscientes de las actividades que realizan.

REFERENCIAS

- Amuntio Gómez, M. A., Candau J., Mañas J. A. 2012. *MAGERIT – version 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de información.* https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html [Última visita 06/10/2017]
- *Pilar Tools.* http://www.pilar-tools.com/doc/v62/help_es/cia/WebHelp/index.html#!1127 [Última visita 07/10/2017]