TFM - SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

INTEGRADOR X

Edgar Muñoz Mercader

ÍNDICE DE CONTENIDOS

1. SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL

Integrador X se va a embarcar en la implantación de un Sistema de Gestión de la Seguridad de la Información, en adelante SGSI, con el objetivo de aportar seguridad al principal negocio de ésta. La Dirección de la organización ha manifestado su apoyo y compromiso con dichos objetivos.

En los siguientes apartados se va a proceder a contextualizar el SGSI dentro de la organización, así como la situación actual de la organización en los ámbitos a tratar en el SGSI.

1.1 Presentación de Integrador X

Integrador X es la empresa de tecnología de un gran grupo empresarial. Integrador X está especializada en la provisión de soluciones digitales y servicios de valor añadido para la Transformación Digital de compañías privadas y Administraciones Públicas.

Centra su experiencia, talento y conocimiento sectorial en el desarrollo de propuestas integrales de valor con base tecnológica, orientadas a maximizar el valor de la relación de las organizaciones optimizando a la vez la operación de su negocio.

Trabaja con los líderes globales del sector y con empresas emergentes, especialistas de cada industria, combinando las mejores capacidades, para conseguir resultados diferenciales en los clientes.

Las máximas de Integrador X son:

- **Cercanía:** Escucha de cerca a los clientes para entender mejor sus necesidades, formando con ellos un equipo sólido en cada uno de los proyectos abordados.
- **Compromiso:** Acompaña a los clientes con la máxima implicación, llevando cada proyecto a alcanzar el resultado esperado, aportando el esfuerzo y recursos necesarios hasta conseguirlo.
- **Continuidad:** Crea relaciones sólidas y duraderas. Su labor no acaba con un proyecto. Avanzan conjuntamente con los clientes en un proceso de actualización y transformación constante.
- **Flexibilidad:** Adaptación con agilidad a las necesidades de sus clientes.

1.1.1 Ejes de Transformación

El modelo de negocio de Integrador X se basa en cuatro ejes de transformación que ofrecen un enfoque integral único y diferencial. Una propuesta completa de soluciones y servicios digitales con visión *end-to-end*, para abordar una Transformación Digital de sus clientes que trasciende a la infraestructura, las aplicaciones de negocio, los datos y por supuesto, el cliente/ciudadano.

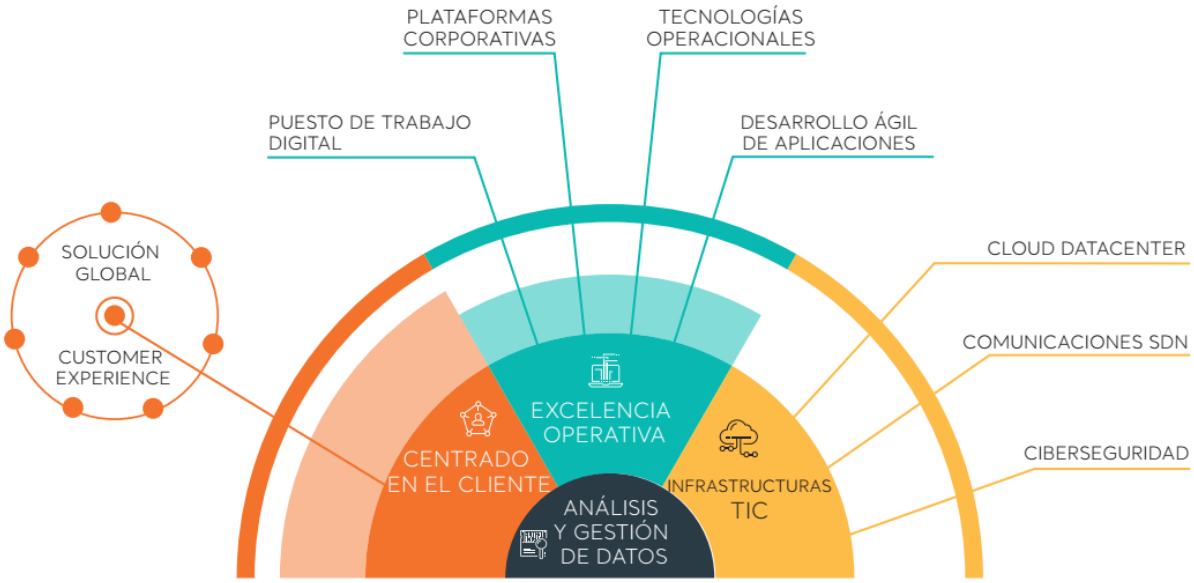


Imagen 1: Ejes de Transformación de Integrador X

Innovación

Un modelo de innovación abierta para resolver, entre todos, los mayores retos de la Transformación Digital. Importando prácticas de éxito de otros lugares del planeta para hacerlos realidad aquí, al lado de sus clientes. Con el impulso de organismos nacionales y europeos, que ayudan a despegar más rápido hacia el nuevo horizonte digital.

1.1.2 Divisiones

Todo el trabajo y actividad está enfocado hacia nuevos modelos de colaboración para orientar a los clientes en las nuevas necesidades de la transformación digital.

La oferta está soportada por cuatro divisiones, en campos concretos de conocimiento, con soluciones que proporcionan nuevos modelos de negocio y de gestión para un mundo digital conectado.

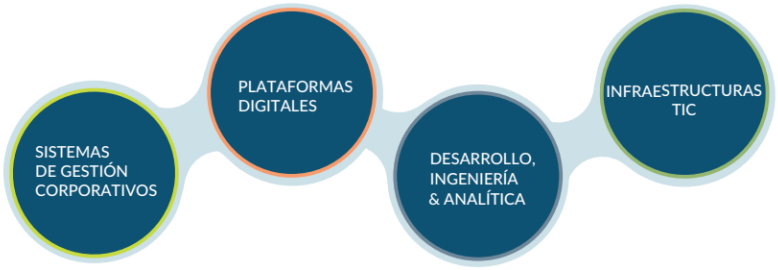


Imagen 2: Divisiones de Integrador X

1.1.3 Sectores de Actividad

Enfoques diferentes para afrontar retos distintos. Adaptan su visión de la Transformación Digital a los desafíos de cada industria y cliente, para conseguir ventajas diferenciales e inimitables. Con una propuesta personalizada y definida desde el conocimiento y experiencia en clientes de múltiples sectores.

- Gobierno y Servicios Públicos
- *Utilities*
- Territorio Inteligente
- Industria
- Turismo
- Transporte
- Banca y Seguros
- *Retail*
- Sanidad
- Educación
- Defensa y Seguridad

1.2 Beneficios, Objetivos y Alcance del SGSI

Los sistemas y procesos que hacen uso de información son, para toda organización, activos de gran importancia y por tanto activos que deben ser protegidos. La protección infinita como tal no existe, ya que siempre hay, o habrá, una vulnerabilidad técnica, un riesgo imposible de mitigar o erradicar, etc. con los que las organizaciones deben convivir y por tanto siempre existe cierto nivel de riesgo.

En una organización la implantación de un SGSI ayuda a definir procedimientos y políticas y a establecer la planificación e implantación de controles de seguridad basados en una evaluación de riesgos previo, siempre alineado con los objetivos de negocio de la organización y con la finalidad de mantener un nivel de riesgo por debajo del umbral que se defina al amparo de este SGSI.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información. Con estos riesgos decide si los asume, los evita, los minimiza, los transfiere o planifica su mitigación mediante la planificación de la implantación de controles.

Historia y Orígenes de las ISO/IEC 27001 y ISO/IEC 27002:

El SGSI planteado va a ser desarrollado utilizando como marco de trabajo la familia de normas ISO/IEC 27000. Las normas ISO/IEC 27000 conforman un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información. Este marco es planteable para cualquier tipo de empresa u organismo ya que plantea una guía que deberá/podrá ser adaptada y particularizada a cada organización.

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution) es responsable de la publicación de importantes normas. Muchas de estas normas han sido referente de futuras normas ISO:

- BS 5750. Publicada en 1979. Origen de ISO 9001
- BS 7750. Publicada en 1992. Origen de ISO 14001
- BS 7799. Publicada en 1995. Origen de ISO/IEC 27000

En el caso que nos ocupa, la ISO/IEC 27000 proviene de la norma BS 7799 de BSI:

- La primera parte de la norma -BS 7799-1- fue una guía de buenas prácticas que, con el paso de los años, fue evolucionando hasta convertirse en la ISO/IEC 27002.
- Es la segunda parte -BS 7799-2-, publicada por primera vez en 1998, la que estableció los requisitos de un SGSI certificable que evolucionó hasta derivar en la ISO/IEC 27001.

1.2.1 Beneficios de la Implantación de un SGSI

La implantación de un SGSI comporta los siguientes beneficios a las organizaciones:

- Visión Global: define las políticas de seguridad de la información que conformarán las bases del resto del SGSI. Dichas políticas de seguridad deberán ser conocidas, aprobadas y promovidas por la Dirección.
- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Implicación de la Organización: para llevar a cabo un SGSI se requiere la implicación de toda la organización: desde la Dirección, hasta el usuario final, definiendo una estructura

de roles y responsabilidades que abarcan a gran parte de la estructura de la organización. Confianza y reglas claras para todas las personas de la organización.

- Gestión Global: define los requerimientos para la gestión de la seguridad de la información desde un punto de vista global, siguiendo criterios comunes y procedimientos homogéneos para todas las áreas implicadas.
- Solución Viva: Un SGSI no finaliza con la implantación de una serie de medidas o controles para gestionar el riesgo de una organización, sino que es un proceso en constante revisión y actualización: Los riesgos y sus controles son continuamente revisados.
- Mejora continua: permite establecer una planificación para ir alcanzando los objetivos en diferentes iteraciones, de forma que el sistema de gestión se va ampliando gradualmente, y permite tener en marcha un proceso de revisión para asegurar que los problemas en iteraciones anteriores se detectan y corrigen en posteriores iteraciones., que se incorporan las lecciones aprendidas en cada nueva iteración y que se implantan mejoras justificadas, permitiendo evolucionar paso a paso.
- Control y seguimiento: permite disponer de una metodología de medida y evaluación mediante indicadores, que permite evaluar los resultados obtenidos frente a los objetivos establecidos y así mantener debidamente informada a la Dirección mediante una visión ejecutiva del sistema. Asimismo, establece los mecanismos de autoevaluación y facilita la realización de auditorías de seguridad de la información cuando corresponda.
- Optimización de los recursos y por tanto reducción de costes:
  - Uso racional y más controlado de la información.
  - Presupuesto justificado, ajustado al riesgo real.
  - Personal concienciado y formado en sus responsabilidades. Aumento de la motivación y satisfacción del personal.
  - Ahorro de tiempo, puesto que los procedimientos y criterios esenciales están claramente definidos y comunicados.
  - Infraestructura ajustada a los riegos detectados y a las necesidades reales del negocio.
- Posibilidad de integración con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001…).
- Conformidad con la legislación vigente relativa a la gestión de la seguridad de la información: información de carácter personal, propiedad intelectual y otras.
- Reconocimiento y elemento diferenciador frente a la competencia: Confianza de clientes, proveedores y socios en general.

1.2.2 Objetivos

El objetivo de la implantación del SGSI a desarrollar en los próximos apartados es principalmente la de aportar un nivel de seguridad adecuado en los procesos de negocio de Integrador X relacionados con la gestión de sus clientes, adecuarse a los requerimientos de seguridad cada vez más demandados por el mercado y trasmitir confianza en las metodologías utilizadas a los clientes de la organización.

1.2.3 Alcance

1.2.3.1 Áreas Organizativas

Principalmente el SGSI se centrará en los procesos relacionados con la actividad de las Áreas Comerciales y de Operaciones. Estas áreas gestionan una serie de información relativa a

oportunidades de negocio, propuestas técnico/económicas, documentación de proyecto, etc., en su gran mayoría, muy vinculada con los clientes de la organización. Es vital para la organización que dicha información sea gestionada aplicando los niveles de seguridad definidos por el Comité de Seguridad y aprobados por la Dirección.

En el siguiente organigrama se muestra de manera esquemática la estructura de Integrador X, en parte, para clarificar los procesos de las áreas implicadas en el SGSI.

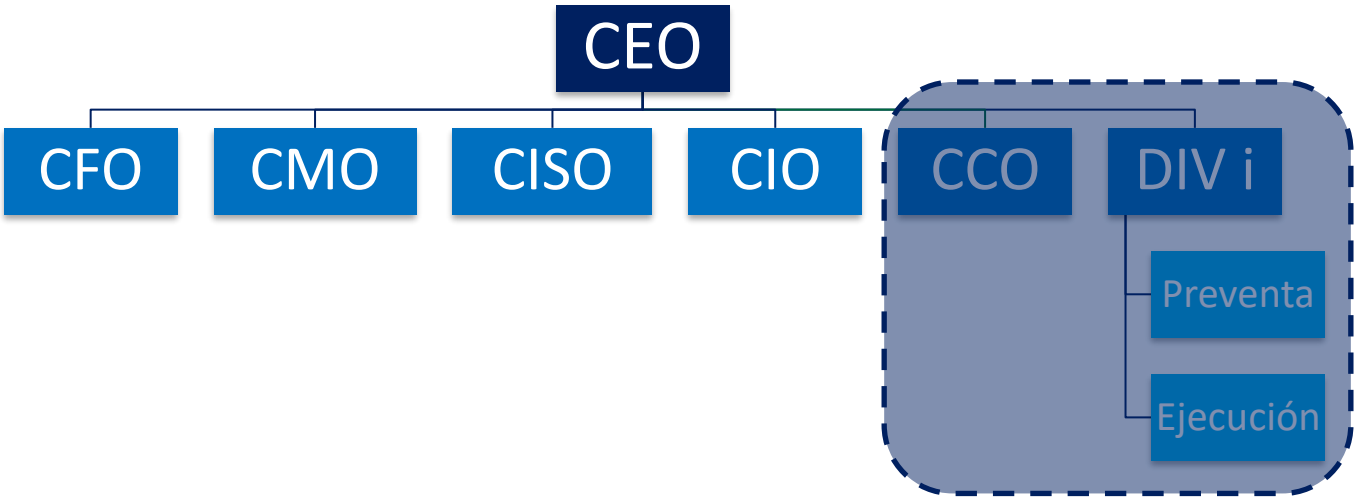


Imagen 3: Alcance Organizativo del SGSI

En el anterior organigrama, se han representado parte de la estructura directiva de Integrador X:

- CEO – *Chief Executive Officer* como máximo responsable de la gestión y dirección administrativa en la empresa.
- CISO - *Chief Information Security Officer* como Gestión de la Seguridad de la Información.
- CIO - *Chief Information Officer* como gerente de sistemas o director de tecnologías de la información, siendo un cargo operacional. En Integrador X no existe la figura de CTO (*Chief Technology Officer*); este rol, similar al del CIO, pero algo más técnico queda asumido por el propio CIO.
- CCO - *Chief Commercial Officer* como máximo responsable comercial de Integrador X y que conforma parte de la Dirección de Integrador X.
  En este ámbito, aunque sin afectación en el SGSI planteado, existen tres responsables comerciales por sector (Administraciones Públicas, Banca y Seguros e Industria). Estos tres responsables conforman parte de la Dirección sin tener un CCO como tal que represente a los tres. Por no añadir complejidad al esquema se ha considerado conveniente no representar los tres responsables.
- DIV i – Directores de cada una de las divisiones (Sistemas de Gestión Corporativos, Plataformas Digitales, Desarrollo, Ingeniería & Analítica e Infraestructuras TIC) como máximos responsables de las diferentes Divisiones de Negocio de Integrador X y que conforma todos ellos parte de la Dirección de Integrador X.
  Estas Divisiones de Negocio se dividen a su vez en un área de Preventa y un área de Ejecución. Estas áreas son independientes entre las diferentes Divisiones, razón por la cual no existe la figura de COO (*Chief Operating Officer*) global presente en otras organizaciones.

- Adicionalmente, a modo de muestra, se han incorporado otras figuras constituyentes del Comité de Dirección pero sin afectación para el SGSI planteado: CMO (*Chief Marketing Officer*) y CFO (*Chief Financial Officer*).

En el anterior esquema se ha remarcado las áreas, los procesos de las cuales, se han contemplado en el SGIS:

- Áreas Comerciales: Áreas bajo responsabilidad del CCO y las diferentes áreas de preventa de las diferentes Divisiones.
- Áreas de Operaciones: Diferentes áreas de ejecución de las diferentes Divisiones.

1.2.3.2 Infraestructuras TI

A nivel de sistemas de Tecnologías de la Información, TI, el ámbito del SGSI será el utilizado por las áreas anteriormente indicadas. En el siguiente esquema se puede observar de una manera esquemática los sistemas TI implicados en los procesos de las Áreas Comerciales y de Operaciones.

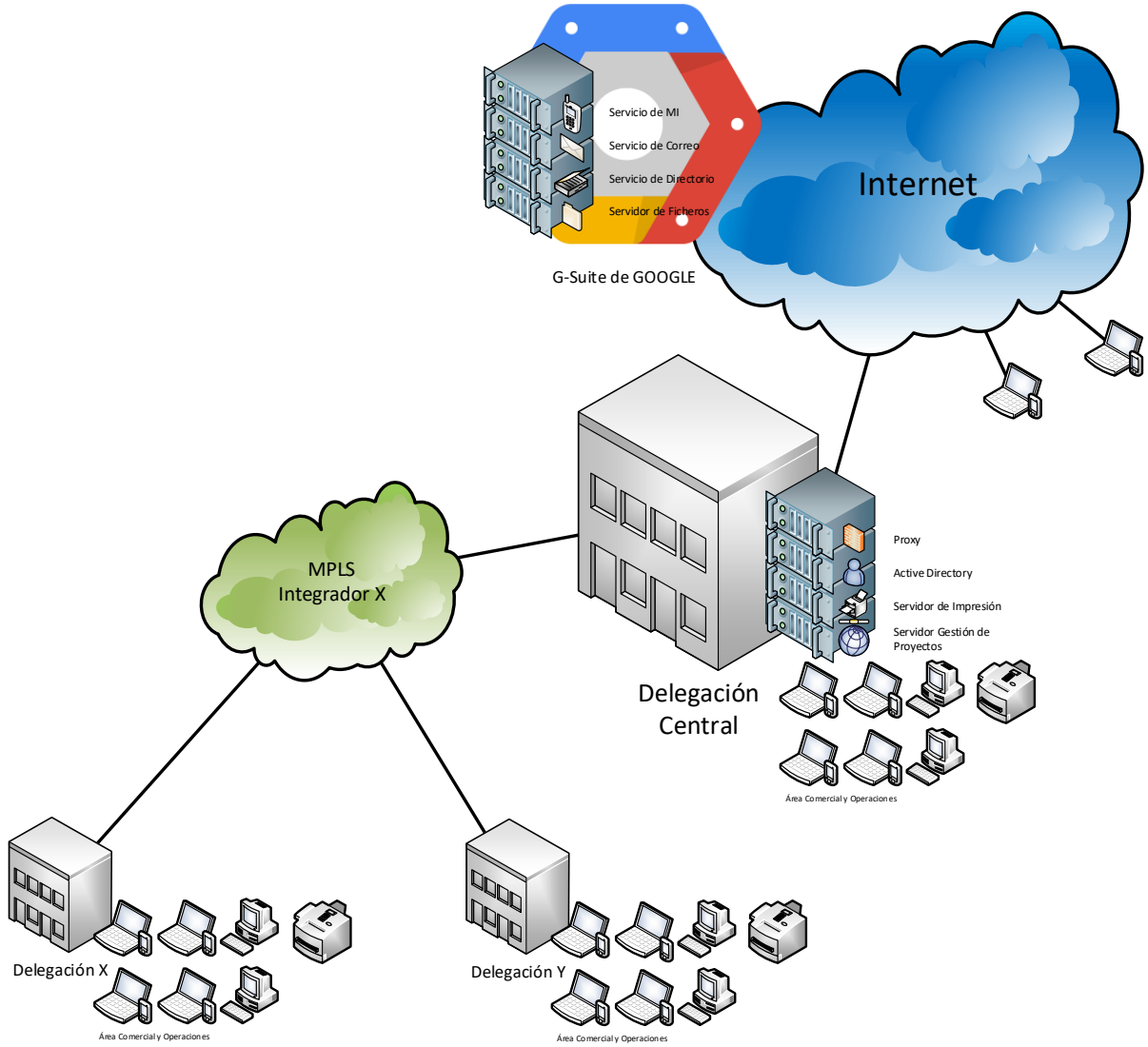


Imagen 4: Alcance TI del SGSI

Las áreas Comercial y de Operaciones, a pesar de ser coordinadas desde la delegación central, desarrollan sus funciones de manera distribuida en el territorio. A nivel de

comunicaciones las diferentes delegaciones están interconectadas entre si a través de una red MPLS privada para Integrador X. Gracias a esta interconexión, la totalidad de los empleados trabajan con los Sistemas de Información (SI) de manera homogénea. De manera adicional, determinados perfiles (Comerciales, Consultores de Venta -CVs- y Jefes de Proyecto -JPs) pueden teletrabajar con los sistemas de la organización siempre que dispongan de conexión a Internet. Esto es posible gracias a la posibilidad de establecer comunicaciones VPN con la delegación central.

A nivel de SI, la organización dispone de dos entornos:

- Un entorno *on-premise*, en las propias dependencias de la organización, desde donde se prestan determinados servicios a los empleados como son:
  - Servicio de gestión de identidades para a autenticación de los usuarios que desean acceder a los SI.
  - Servicio de navegación segura a Internet.
  - Servicio de protección anti-virus, anti-malware, etc.
  - Servicio de gestión impresión optimizada.
  - Servicio de Gestión de Proyectos.
- Un entorno en el *cloud*, desde donde se prestan determinados servicios. Estos servicios son prestados a través de la solución comercial G-Suite de GOOGLE. Estos servicios son, principalmente:
  - Servicio de correo electrónico.
  - Servicio de *file storage*.
  - Servicio de mensajería instantánea (MI).
  - Servicio de directorio corporativo.
  - Servicio de agenda (calendario).

La mayoría de empleados de las Áreas Comerciales y de Operaciones, su equipo de trabajo más habitual es un equipo portátil (laptop) y un smartphone con tarifa de datos habilitada. A través del equipo portátil los empleados disponen de acceso a la totalidad de los servicios necesarios para el desarrollo de sus funciones, en cambio, a través del smartphone se dispone de acceso sólo a determinados servicios: principalmente aquellos prestados a través de la plataforma G-Suite: Gmail, Google Drive, Hangouts, Contactos, Calendario, etc.

1.3 Análisis Diferencial

El Análisis Diferencial, o Análisis GAP, de Integrador X que se expone en el presente apartado permitirá conocer la situación actual de la organización con respecto a la normativa ISO/IEC 27001:2013 y los controles enunciados en el Anexo A de esta misma norma, y más ampliamente desarrollados en la norma ISO/IEC 27002:2013.

1.3.1 Requerimientos ISO/IEC 27001

La ISO/IEC 27001 define 7 grupos de requerimientos para establecer, implementar, mantener y mejorar de manera continua un SGSI en una organización. El cumplimiento de estos requerimientos es imprescindible para la conformidad de una organización con dicho estándar internacional.

La situación actual de Integrador X en relación con estos requerimientos es el que se detalla en los siguientes apartados.

1.3.1.1 Contexto de la Organización

- Entendimiento de la organización y su contexto: Integrador X es perfectamente conocedora de su modelo de negocio y como la gestión de la seguridad de información relativa a los procesos de las Áreas Comerciales y de Operaciones es imprescindible para el correcto funcionamiento de la organización.
- Entendimiento de las necesidades y expectativas de las partes interesadas: Integrador X tiene identificadas las partes interesadas y sus expectativas en la gestión de la seguridad de la información. Estas partes interesadas son, en primera instancia, los empleados de Integrador X generadores/consumidores de esta información y de ahí, toda la cadena de mando hasta la misma Dirección. Las principales expectativas de las partes interesadas son que exista una gestión de la seguridad de la información que prevenga la revelación o un uso fraudulento de la información gestionada por las Áreas Comerciales y de Operaciones.
- Definición del alcance del SGSI: El alcance del SGSI planteado, tal y como se ha enunciado en el anterior punto (0), son los procesos relacionados con la actividad de las Áreas Comerciales y de Operaciones y la información relacionada con éstos.
- Sistema de Gestión de la Seguridad de la Información: Integrador X se encuentra en una fase temprana de la implementación de un SGSI. En la actualidad no existe un SGSI para el contexto y alcance definido en los puntos anteriores.

1.3.1.2 Liderazgo

- Liderazgo y compromiso: Si bien la actual Dirección de Integrador X no se ha pronunciado explícitamente al respecto del SGSI planteado en el presente documento, si ha revelado su convencimiento de la importancia de la Seguridad de la Información, de su necesidad y del alineamiento de ésta con los objetivos de negocio de la organización. Muestra de ello es la reciente creación de la figura del CISO -el pasado año 2017- y la creación de un Comité de Seguridad para la gestión de los temas relacionados con la Seguridad de la Información.
- Políticas de Seguridad de la Información: Se desconoce la existencia o no de una política de seguridad corporativa ni la periodicidad de revisión de ésta, en el caso de existir.
- Roles organizativos, responsabilidades y autoridades: Se desconoce si existe una asignación de roles, responsabilidades y autoridades relativas a la Seguridad de la Información.

1.3.1.3 Planificación

- Acciones para la gestión de riesgos y oportunidades: Se desconoce si Integrador X ha realizado un análisis y gestión de riesgos concreto para el ámbito del SGSI planteado. Si se han realizado

determinadas iniciativas en el ámbito de la Seguridad de la Información, pero se desconoce si estas iniciativas son derivadas de un análisis de riesgos previo.

- Definición de objetivos en la Seguridad de la Información y planificación para su consecución: Se desconoce si se han definido una serie de objetivos en el ámbito de la Seguridad de la Información y se desconoce, por tanto, si existe una planificación para su consecución.

1.3.1.4 Soporte

- Recursos: Tal y como se ha comentado en puntos anteriores, el pasado año la organización creó la figura del CISO y un Comité de Seguridad. Adicionalmente, bajo la responsabilidad del CISO, se ha creado una estructura a la que se le ha asignado una partida presupuestaria.
- Competencia: La estructura creada bajo responsabilidad del CISO está conformada por profesionales del ámbito de la seguridad poseedores de titulaciones de amplio reconocimiento en el sector y de certificaciones de los principales fabricantes de soluciones de seguridad del mercado.
- Concienciación: El Departamento de Seguridad ha realizado y realiza acciones de concienciación relativas a la seguridad de la información. Al poco de la creación del departamento se realizaron unas sesiones de concienciación de obligada asistencia para todo el personal del a organización y de todas las delegaciones. Por otro lado, mediante acciones puntuales, se recuerda a los empleados determinados aspectos relativos a la seguridad de la información: renovación y actualización de la protección de anti-virus/anti-malware de los puestos de trabajo, instalación de un producto para el borrado seguro de la información, etc.
- Comunicación: Como se ha comentado en el punto anterior, tras la creación del Departamento de Seguridad, se realizaron, a la totalidad de los empleados de la organización, unas sesiones de concienciación relativas a la seguridad de la información. Estas sesiones fueron de asistencia obligada y fueron realizadas varias sesiones para la totalidad de delegaciones del territorio nacional, para facilitar al máximo la asistencia del personal interno. Algunas de estas sesiones fueron grabadas y puestas a disposición del personal para su posterior visualización.

  No se tiene constancia de ningún tipo de comunicación hacia el exterior o a personal externo que desarrolla sus funciones en las dependencias de Integrador X.
- Documentación: En la actualidad no existe documentación relativa a la aplicación del SGSI planteado en el presente documento y se desconoce de la existencia de cualquier otro tipo de documentación relativa a la seguridad tal y como define la ISO/IEC 27001-2013.

1.3.1.5 Operación

- Planificación y Control Operacional: En la actualidad no existe una definición de los procesos requeridos por el SGSI definido en el presente documento por estar éstos en fase de definición.
- Evaluación de Riesgos asociados a la Seguridad de la Información: Se desconoce si se ha realizado una evaluación de riesgos asociados a la Seguridad de la Información. En el ámbito del SGSI presentado en el presente documento este análisis de riesgos no se ha realizado.
- Gestión de Riesgos asociados a la Seguridad de la Información: Se desconoce si se ha realizado una gestión de riesgos asociados a la Seguridad de la Información. En el ámbito del SGSI presentado en el presente documento, al igual que para la evaluación de riesgos, esta gestión de riesgos no se ha realizado.

1.3.1.6 Evaluación del funcionamiento

- Monitorización, medida, análisis y evaluación: No se tiene constancia de que la organización esté monitorizando el funcionamiento de ningún SGSI; el SGSI en proceso de definición en el presente documento tampoco por estar, precisamente, en fase de definición.
- Auditorías Internas: La organización, a raíz de la creación del Departamento de Seguridad, está realizando auditorías de seguridad, aparentemente aleatorias, para determinados proyectos en ejecución (dentro del ámbito del Área de Operaciones).

- Revisión por parte de la Dirección: Se desconoce si la Dirección, en la actualidad, está llevando a cabo revisiones de los SGSI implantados. El SGSI en definición en el presente documento no está siendo revisado por la Dirección.

1.3.1.7 Mejora continua

- No-conformidades y Acciones Correctoras: Se desconoce si se están llevando a cabo la revisión de no-conformidades, ni la aplicación de acciones correctoras. Desde el punto de vista del empleado se observan acciones en el ámbito de la Seguridad de la Información, pero se desconoce si estas son derivadas de acciones correctoras y/o revisión de no-conformidades.
- Mejora continua: Se desconoce si la organización está aplicando un proceso de mejora continua. Como se ha comentado en el anterior punto, desde el punto de vista del empleado se observan acciones en el ámbito de la Seguridad de la Información, pero se desconoce si estas son derivadas una política de mejora continua en ejecución dentro de Integrador X.

A continuación, se muestra gráficamente el estado de madurez de cada uno de los requisitos anteriores. El nivel de madurez se ha realizado en base a los niveles definidos por CMM[1]. CMM define 5 niveles y es útil para la evaluación de la seguridad en base a estos niveles y no en base a objetivos concretos. Los niveles y su traslación al mundo de la Seguridad de la Información es el que se muestra en la siguiente tabla.

Valoración	Nivel CMM	Nivel ISO/IEC 27000
0	Inexistente	Ausencia completa del control/requisitos
1	Inicial	Existe una evidencia de que el problema existe y necesita ser gestionado. Aun así, no existe tratamiento no existe tratamiento para éste.
2	Reproducible	El control/requisito de seguridad se encuentra en desarrollo con documentación incompleta
3	Definido	Existe documentación y comunicación relativa al control/requisito, pero no se realiza un seguimiento más allá del realizado a nivel individual.
4	Gestionado	Es posible monitorizar y medir la/el efectividad/cumplimiento del control/requisito pero no está completamente automatizado.
5	Optimizado	El control/requisito ha sido refinado como resultado de la mejora continua del SGSI

Tabla 1: Nivel de madurez ISO/IEC 27000 según CMM

[1] CMM (Capability Maturity Model): Es un modelo de evaluación de los procesos de una organización que proporciona información del nivel de madurez de los controles implementados según el modelo 0: Inexistente; 1: Inicial; 2: Reproducible; 3: Definido; 4: Gestionado ó 5: Optimizado.

El diagrama radial donde se representa el grado de madurez de cada uno de los requerimientos en función de los niveles definidos por CMM es el mostrado a continuación.

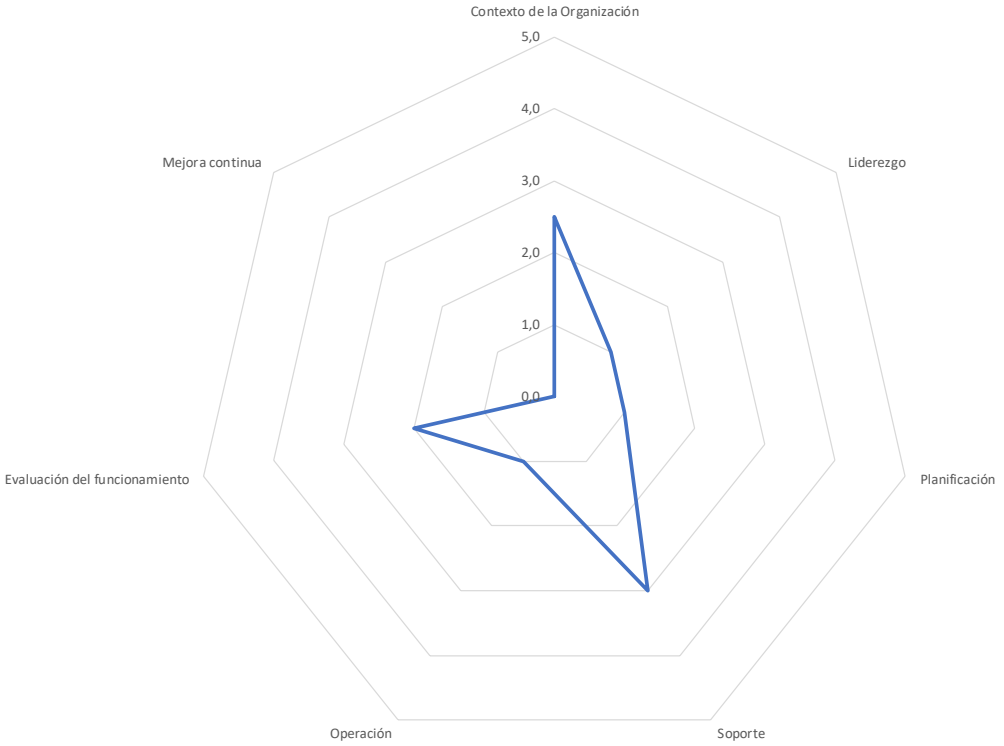


Imagen 5: Grado de madurez de los requisitos de la ISO/IEC 27001

Este gráfico ha sido realizado promediando para cada uno de los requisitos los sub-requisitos contenidos en éste tal y como se detalla en la siguiente tabla.

Requisitos	**Requisito promedio**	**Sub-requisitos**				
Contexto de la Organización	2,5	3	3	3	1	
Liderazgo	1,0	3	0	0		
Planificación	1,0	2	0			
Soporte	3,0	3	3	4	4	1
Operación	1,0	1	1	1		
Evaluación del funcionamiento	2,0	1	4	1		
Mejora continua	0,0	0	0			

Tabla 2: Cumplimiento requisitos ISO/IEC 27001

A continuación se muestra la distribución en el grado de madurez de los diferentes requerimientos según el anterior detalle.

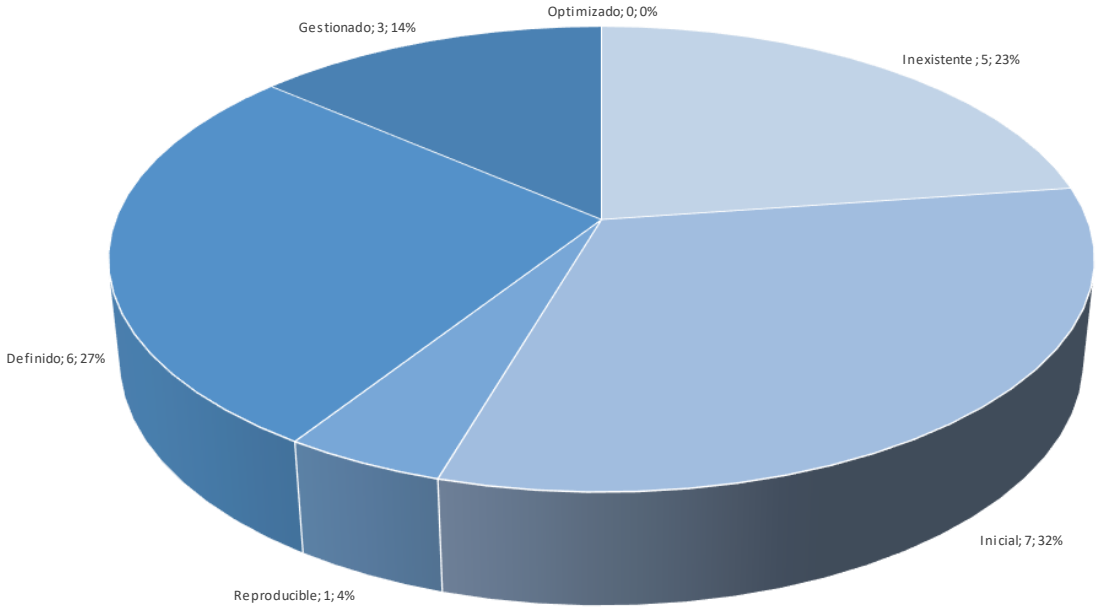


Imagen 6: Requerimientos ISO/IEC 27001 - Distribución según el grado de madurez

1.3.2 Controles ISO/IEC 27002

A parte de los requerimientos definidos en la ISO/IEC 27001, la ISO/IEC 27002:2013 establece 14 dominios con un total de 35 categorías principales. A su vez, para cada una de estas 35 categorías de control se especifican el/los objetivo/s de control y una o más acciones para conseguir dicho objetivo (control/es), en total la ISO/IEC 27002:2013 define 114 controles.

Estos objetivos propuestos por la ISO/IEC, son una propuesta. En función de cada organización, de la actividad principal de ésta, del modelo para llevar a cabo sus actividades, de su estructura, de la situación inicial en el ámbito de la seguridad, etc. serán de aplicación unos u otros objetivos. En este sentido la norma debe ser considerada como una referencia a la hora de seleccionar controles dentro del proceso de implantación de un SGSI.

En el caso de Integrador X la situación actual en el ámbito de la Seguridad de la Información, en relación con los controles definidos en la ISO/IEC 27002:2013 es el que se define a continuación[2]:

5. Políticas de seguridad de la información

5.1. Directrices de la Dirección en seguridad de la información: Se desconoce si existe un conjunto de políticas para la Seguridad de la Información.

[2] En el caso de no comentarse nada explícitamente para una Categoría o un Control, para esta Categoría o Control aplica el comentario jerárquicamente superior, del Capítulo o Categoría, respectivamente.

5.1.1. Políticas para la seguridad de la información
5.1.2. Revisión de las políticas para la seguridad de la información

6. Organización de la seguridad de la información

6.1. Organización Interna: Se desconoce cómo se organiza la Seguridad de la Información en la organización.

6.1.1. Roles y responsabilidades en Seguridad de la Información
6.1.2. Segregación de tareas
6.1.3. Contacto con las autoridades
6.1.4. Contacto con grupos de interés especial
6.1.5. Seguridad de la Información en la gestión de proyectos: En este ámbito existen iniciativas, desde la ceración del Departamento de Seguridad, que velan por la Seguridad de la Información de los proyectos ejecutados desde el Área de Operaciones de Integrador X. Estas iniciativas son, principalmente:
- Auditorías aleatorias sobre proyectos en ejecución.
- Establecimiento de requerimientos de seguridad que deberán ser cumplidos en base a una categorización inicial realizada por el Consultor de Venta, en adelante CV, en el Área Comercial, o por el Jefe de Proyecte, en adelante JP, en el Área de Operaciones.

6.2. Los dispositivos móviles y el teletrabajo

6.2.1. Política de dispositivos móviles: Existen dispositivos móviles, estos están gestionados por una plataforma de gestión de dispositivos móviles centralizada (MDM: Mobile Device Management), pero se desconoce que políticas de seguridad se aplican a los dispositivos. En la actualidad no se están realizando bloqueos en la navegación, descargas, etc., visiblemente no se aprecia ningún anti-virus instalado, etc.
6.2.2. Teletrabajo: Integrador X, para determinados perfiles de empleados, permite el teletrabajo y dota a los empleados de herramientas para el desarrollo de sus funciones habituales sin necesidad de estar físicamente en su puesto de trabajo. Estas herramientas son:
- la utilización herramientas en el *cloud* disponibles desde cualquier ubicación con acceso a Internet: correo electrónico, almacenamiento corporativo, calendario, contactos, etc. a través de G-Suite de GOOGLE.
- y un software para la conexión remota VPN de los empleados a la organización

7. Seguridad relativa a los recursos humanos

7.1. Antes del empleo

7.1.1. Investigación de antecedentes: Se desconoce si la empresa realiza una investigación de los antecedentes de un candidato de manera previa a su contratación.
7.1.2. Términos y condiciones del empleo: Previo a la firma del contrato laboral, o como parte de las cláusulas de éste, se informa al nuevo empleado, de una manera genérica, de los requerimientos de Seguridad de la Información que tiene la organización: confidencialidad de la información, propiedad de Integrador X, etc.

7.2. Durante el empleo

7.2.1. Responsabilidades de gestión: No se realizan gestiones explicitas para asegurar del cumplimiento de las políticas y procedimientos establecidos; en parte porque, tal y como se ha indicado en el punto 5 del presente listado, se desconoce de la existencia de dichas políticas y de sus contenidos.
7.2.2. Concienciación, educación y capacitación en seguridad de la información: Desde la creación del Departamento de Seguridad se han realizado diversas acciones de formación y concienciación en el ámbito de la seguridad. La asistencia a estas acciones fue de obligado cumplimiento para la totalidad de los empleados internos.

7.2.3. Proceso disciplinario: Se desconoce de la existencia de un proceso disciplinario formal a ejecutar ante una violación de las políticas de seguridad definidas.

7.3. Finalización del empleo o cambio de puesto de trabajo

7.3.1. Responsabilidades ante una finalización o cambio: No se tiene constancia de ningún tipo de comunicación relativa a cambios de responsabilidades en el ámbito de la Seguridad de la Información ante un cambio en el rol/responsabilidad de un empleado.
Ante la finalización de la relación laboral de un empleado con Integrador X, se desconoce si existe un procedimiento de baja ordenada de las credenciales de acceso de este empleado a los sistemas de información de la organización.

8. Gestión de activos

8.1. Responsabilidad sobre los activos: Se desconoce la gestión que realiza la organización al respecto de los activos, sus propietarios, etc.

8.1.1. Inventario de activos
8.1.2. Propiedad de los activos
8.1.3. Uso aceptable de los activos
8.1.4. Devolución de activos

8.2. Clasificación de la información: Se desconoce si existe una clasificación de la información definida; si existe, ésta no está siendo aplicada.

8.2.1. Clasificación de la información
8.2.2. Etiquetado de la información
8.2.3. Manipulado de la información

8.3. Manipulación de soportes: No existen, o no se están aplicando, procedimientos para la gestión de soportes extraíbles.

8.3.1. Gestión de soportes extraíbles
8.3.2. Eliminación de soportes
8.3.3. Soportes físicos en tránsito

9. Control de acceso

9.1. Requisitos de negocio para el control de acceso

9.1.1. Política de control de acceso: Desde el punto de vista físico, existe una política de control de acceso. Ésta varía en función de la delegación:

- en la delegación central el acceso de los empleados y personal externo está controlado mediante lectores de tarjetas magnéticas que controlan unos tornos de acceso según la persona dispone de acceso o no al centro
- en el resto de delegaciones el acceso de los empleados y personal externo se realiza tecleando un código de acceso en la puerta de entrada al centro. Este código es el mismo para todos los empleados internos y difiere del código utilizado por los empleados externos, que es, igualmente, el mismo para todos los casos.

Una vez en el interior del recinto los empleados internos y externos se diferencian en función del color de la cinta donde se debe colgar la tarjeta identificativa de cada empleado.

9.1.2. Acceso a las redes y a los servicios de red: Existe un sistema de gestión de identidades que gestiona los datos de acceso de los diferentes empleados, internos y externos, y si estos disponen de los permisos necesarios para acceder o no a los diferentes activos.

9.2. Gestión de acceso de usuario

9.2.1. Registro y baja de usuario: Existe un procedimiento por el cual se provisionan y eliminan usuarios del sistema de gestión de identidades. Se desconocen los detalles de dicho procedimiento.

9.2.2. Provisión de acceso de usuario: Existe un procedimiento por el cual se asignan o revocan derechos de acceso de los usuarios. Se desconocen los detalles de dicho procedimiento.

9.2.3. Gestión de privilegios de acceso: Se desconoce su existencia.

9.2.4. Gestión de la información secreta de autenticación de los usuarios: Se desconoce si la asignación de información secreta de autenticación está procedimentada. En función de las necesidades el operador de atención al usuario (CAU) puede actuar de maneras diversas.

9.2.5. Revisión de los derechos de acceso de usuario: Se desconoce su existencia.

9.2.6. Retirada o reasignación de los derechos de acceso: Se desconoce su existencia.

9.3. Responsabilidades del usuario

9.3.1. Uso de la información secreta de autenticación: Los usuarios utilizan las prácticas marcadas para el uso de la información secreta de autenticación.

9.4. Control de acceso a sistemas y aplicaciones

9.4.1. Restricción del acceso a la información: Los usuarios, debidamente autenticados, sólo pueden acceder a la información y aplicaciones (y sus funciones) para las que se le ha proporcionado acceso.

9.4.2. Proceso seguro de inicio de sesión: El proceso de inicio de sesión actual es mediante usuario y contraseña.

9.4.3. Sistema de gestión de contraseñas: Existe una política y herramientas de control para el uso de contraseñas seguras y robustas.

9.4.4. Uso de utilidades con privilegios del sistema: Se desconoce si se está llevando a cabo un control sobre utilidades con privilegios del sistema.

9.4.5. Control de acceso al código fuente de los programas: Se desconoce si se está llevando a cabo este control de acceso.

10. Criptografía

10.1. Controles criptográficos

10.1.1. Política de uso de los controles criptográficos: Existe una política para el cifrado explícito de documentos confidenciales previo a su envío por correo electrónico u otros medios.
Se desconoce si existen otras políticas relacionadas con el cifrado de los dispositivos de los usuarios, unidades de red, etc. Si la hay, esta no se está aplicando en la actualidad.

10.1.2. Gestión de claves: Al igual que en el punto anterior, se desconoce si hay una política relacionada.

11. Seguridad física y del entorno

11.1. Áreas seguras

11.1.1. Perímetro de seguridad física: A nivel de organización, existe un control de acceso basado en la introducción de un código genérico (existen dos códigos: uno para empleados internos y otro para empleados externos) en delegaciones. En la delegación central el acceso es mediante tarjeta de empleado que permite o deniega el acceso a través de unos tornos.
El acceso a zonas que requieren mayor de seguridad: CPDs, salas técnicas, despachos, etc., está controlado mediante diversos métodos: lectores de tarjetas identificativas, cerraduras tradicionales de las que sólo determinado personal dispone de la llave, etc.

11.1.2. Controles físicos de entrada: Los controles físicos de entrada son los comentados en el anterior punto.

11.1.3. Seguridad de oficinas, despachos y recursos: La seguridad aplicada es la descrita en el punto 11.1.1.

11.1.4. Protección contra amenazas externas y ambientales: Existe un plan de emergencia genérico a seguir en caso de incendio. Se desconocen las medidas existentes contra otras amenazas.

11.1.5. El trabajo en áreas seguras: Se desconoce su existencia.

- 11.1.6. Áreas de carga y descarga: Se desconoce su existencia.

11.2. **Seguridad de los equipos:** Se desconoce su existencia.

- 11.2.1. Emplazamiento y protección de equipos
- 11.2.2. Instalaciones de suministro: Existen protecciones contra los fallos en los sistemas de alimentación eléctrica para los equipos ubicados en el CPD. El resto de equipamiento no cuenta con estas protecciones.
- 11.2.3. Seguridad de cableado
- 11.2.4. Mantenimiento de equipos: Existe un servicio de soporte local ante incidencias de los usuarios.
- 11.2.5. Retirada de materiales propiedad de la empresa
- 11.2.6. Seguridad de los equipos fuera de las instalaciones: Los equipos de usuario, fuera de las dependencias de la organización, disponen de los mismos sistemas de protección que cuando estos están dentro. Esto no aplica a los controles aplicados a la navegación.
- 11.2.7. Reutilización o eliminación segura de equipos
- 11.2.8. Equipo de usuario desatendido: Por defecto, los equipos se bloquean de manera automática tras un periodo de inactividad.
- 11.2.9. Política de puesto de trabajo despejado y pantalla limpia: En las sesiones de formación/concienciación se realiza hincapié en este aspecto. A la práctica esta política es aplicada en función de cada usuario.

12. Seguridad de las operaciones

12.1. **Procedimientos y responsabilidades operacionales:** Existe un proyecto para la implantación de una metodología de gestión de proyectos. Esta metodología ha sido desarrollada por Integrador X en base a su experiencia y teniendo en cuenta normativas, estándares de mercados y guías de buenas prácticas como son: ISO9001, ISO20000, ISO27001, CMMI, ITIL, etc. Esta metodología cubre los controles anidados dentro de la presente categoría.

- 12.1.1. Documentación de procedimientos de la operación
- 12.1.2. Gestión de cambios
- 12.1.3. Gestión de capacidades
- 12.1.4. Separación de los recursos de desarrollo, pruebas y operación

12.2. **Protección contra el software malicioso**

- 12.2.1. Controles contra el código malicioso: Existen sistemas para la protección frente a software malicioso. Estas protecciones se aplican tanto en los propios puestos de trabajo, como de manera global en forma de controles perimetrales.

12.3. **Copias de seguridad:** Se desconoce su existencia

- 12.3.1. Copias de Seguridad de la Información: El sistema de almacenamiento corporativo es el almacenamiento en el *cloud* de G-Suite de GOOGLE. Este servicio dispone de políticas de copias de seguridad, aunque se desconocen los detalles de éstas.

12.4. **Registros y supervisión:** Se desconoce su existencia.

- 12.4.1. Registro de eventos
- 12.4.2. Protección de la información de registro
- 12.4.3. Registros de administración y operación
- 12.4.4. Sincronización del reloj

12.5. **Control del software en explotación**

- 12.5.1. Instalación del software en explotación: Se desconoce su existencia.

12.6. **Gestión de vulnerabilidades técnicas:** Se desconoce su existencia

- 12.6.1. Gestión de las vulnerabilidades técnicas

12.6.2. Restricción en la instalación de software: No existe dicha restricción, los usuarios disponen de privilegios para la instalación de software sobre sus equipos.

12.7. **Consideraciones sobre la auditoría de Sistemas de Información**

12.7.1. Controles de auditoría de sistemas operativos: Se desconoce su existencia.

13. **Seguridad de las comunicaciones**

13.1. **Gestión de la seguridad de redes:** Las redes están administradas por personal interno. Se desconoce si se aplica alguna política para la protección de la seguridad de la información.

13.1.1. Controles de red

13.1.2. Seguridad de los servicios de red

13.1.3. Segregación en redes

13.2. **Intercambio de información:** Se desconoce su existencia.

13.2.1. Políticas y procedimientos de intercambio de información

13.2.2. Acuerdos de intercambio de información

13.2.3. Mensajería electrónica

13.2.4. Acuerdos de confidencialidad o no revelación

14. **Adquisición, desarrollo y mantenimiento de los sistemas de información**

14.1. **Requisitos de seguridad en sistemas de información:** Se desconoce su existencia. Los sistemas de información utilizados por Integrador X son productos comerciales.

14.1.1. Análisis de requisitos y especificaciones de seguridad de la información

14.1.2. Asegurar los servicios de aplicaciones en redes públicas

14.1.3. Protección de las transacciones de servicios de aplicaciones

14.2. **Seguridad en el desarrollo y en los procesos de soporte:** Como se ha comentado en 12.1 existe un proyecto para la implantación de una metodología de gestión de proyectos. Esta metodología ha sido desarrollada por Integrador X en base a su experiencia y contempla los controles incluidos en la presente categoría.

14.2.1. Política de desarrollo seguro

14.2.2. Procedimiento de control de cambios en sistemas

14.2.3. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

14.2.4. Restricciones a los cambios en los paquetes de software

14.2.5. Principios de ingeniería de sistemas seguros

14.2.6. Entorno de desarrollo seguro

14.2.7. Externalización del desarrollo de software

14.2.8. Pruebas funcionales de seguridad de sistemas

14.2.9. Pruebas de aceptación de sistemas

14.3. **Datos de prueba:** A priori, no aplica la presente categoría al escenario de Integrador X.

14.3.1. Protección de los datos de prueba

15. **Relación con proveedores**

15.1. **Seguridad en las relaciones con proveedores:** Existe un clausulado estándar, utilizado en todo contrato establecido con proveedores externos a la organización. Aun así, a criterio del responsable del proyecto/operación en Integrador X, es posible ampliar este clausulado según las casuísticas particulares de cada caso.

15.1.1. Política de seguridad de la información en las relaciones con los proveedores

15.1.2. Requisitos de seguridad en contratos con terceros

15.1.3. Cadena de suministro de tecnología de la información u de las comunicaciones

15.2. **Gestión de la provisión de servicios del proveedor:** Como se ha comentado en 12.1 y en 14.2 existe un proyecto para la implantación de una metodología de gestión

de proyectos. Esta metodología contempla los controles incluidos en la presente categoría.

15.2.1. Control y revisión de la provisión de servicios del proveedor

15.2.2. Gestión de cambios en la provisión del servicio del proveedor

16. Gestión de incidentes de seguridad de la información

16.1. **Gestión de incidentes de seguridad de la información y mejoras:** La interlocución de los usuarios con el departamento de Seguridad de Integrador X es a través de un CAU. Éste es responsable de tomar las medidas oportunas ante un incidente asignando cada caso al equipo resolutor oportuno y teniendo a su disposición, por si fuera requerido, una cadena de escalado.

16.1.1. Responsabilidades y procedimientos: Estos están definidos y son conocidos por el CAU para la asignación de los incidentes y/o escalado en función del caso.

16.1.2. Notificación de los eventos de seguridad de la información: Siempre a través del CAU.

16.1.3. Notificación de puntos débiles de la seguridad: En el caso de detectarse un punto débil en la seguridad de la información, éste debe ser notificado al CAU para su gestión oportuna con el equipo resolutor pertinente.

16.1.4. Evaluación y decisión sobre los eventos de seguridad de información: El CAU dispone de los procedimientos pertinentes para la toma de estas decisiones.

16.1.5. Respuesta a incidentes de seguridad de la información: Cada equipo resolutor dispone de los procedimientos a seguir en cada caso.

16.1.6. Aprendizaje de los incidentes de seguridad de la información: Existe una gestión de problemas y una gestión de la base de datos del conocimiento que permite incorporar información relativa a incidentes pasados.

16.1.7. Recopilación de evidencias: Se desconoce su existencia.

17. Aspectos de seguridad de la información para la gestión de la continuidad del negocio

17.1. **Continuidad de la seguridad de la información:** Se desconoce su existencia.

17.1.1. Planificación de la continuidad de la seguridad de la información

17.1.2. Implementar la continuidad de la seguridad de la información

17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información

17.2. **Redundancias**

17.2.1. Disponibilidad de los recursos de tratamiento de la información: Los principales recursos de tratamiento de la información utilizados por Integrador X son de la G-Suite de GOOGLE, un servicio en el *cloud* con mecanismos de redundancia y alta disponibilidad que cubren los requerimientos de la organización.

18. Cumplimiento

18.1. **Cumplimiento de los requisitos legales y contractuales:** En Integrador X existe un Departamento de asesoría jurídica encargado de gestionar los controles incluidos en la presente categoría. Se desconocen los detalles del estado de estos controles.

18.1.1. Identificación de la legislación aplicable y de los requisitos contractuales

18.1.2. Derechos de propiedad intelectual (DPI)

18.1.3. Protección de los registros de la organización

18.1.4. Protección y privacidad de la información de carácter personal: Los empleados han recibido formaciones y sesiones de concienciación específicas sobre esta temática. A la práctica, no se están llevando los controles necesarios para validar el cumplimiento de la normativa por parte de los empleados.

18.1.5. Regulación de los controles criptográficos

18.2. **Revisiones de la seguridad de la información:** Se desconoce su existencia.

18.2.1. Revisión independiente de la seguridad de la información

18.2.2. Cumplimiento de las políticas y normas de seguridad
18.2.3. Comprobación del cumplimiento técnico

A continuación se muestra la distribución en el grado de madurez de los diferentes controles según el anterior detalle.

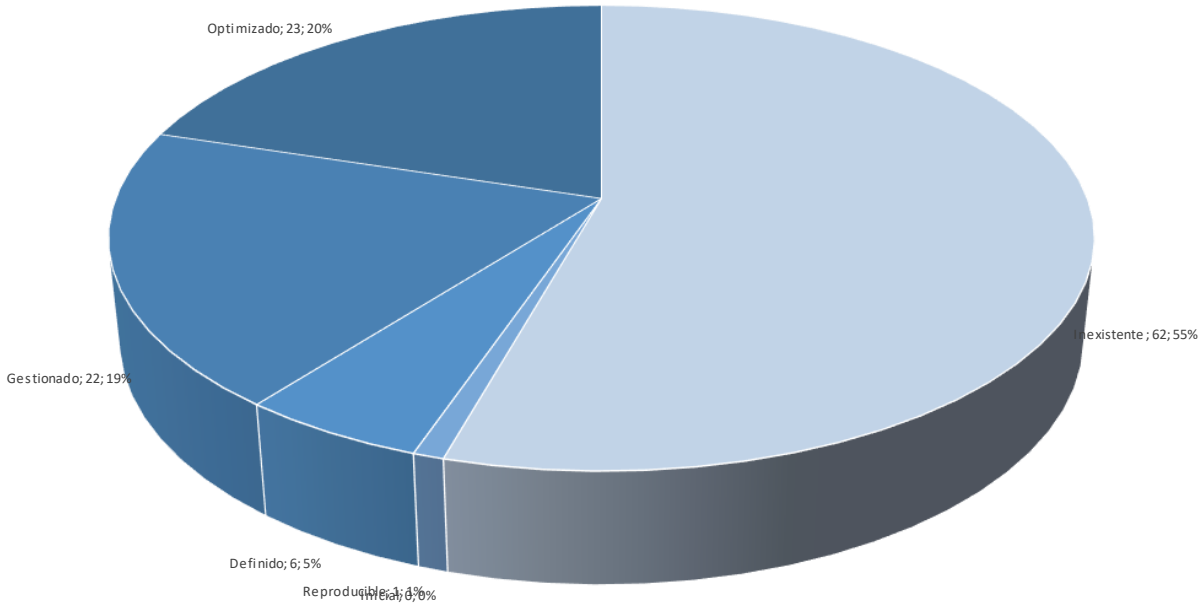


Imagen 7: Controles ISO/IEC 27002 - Distribución según el grado de madurez

A continuación, se muestra gráficamente el estado de madurez de cada uno de los dominios. El nivel de madurez se ha realizado, al igual que se ha realizado para los requisitos planteados por la ISO/IEC 27001 expuesta en el punto anterior (5.8.1), en base a los niveles definidos por CMM.

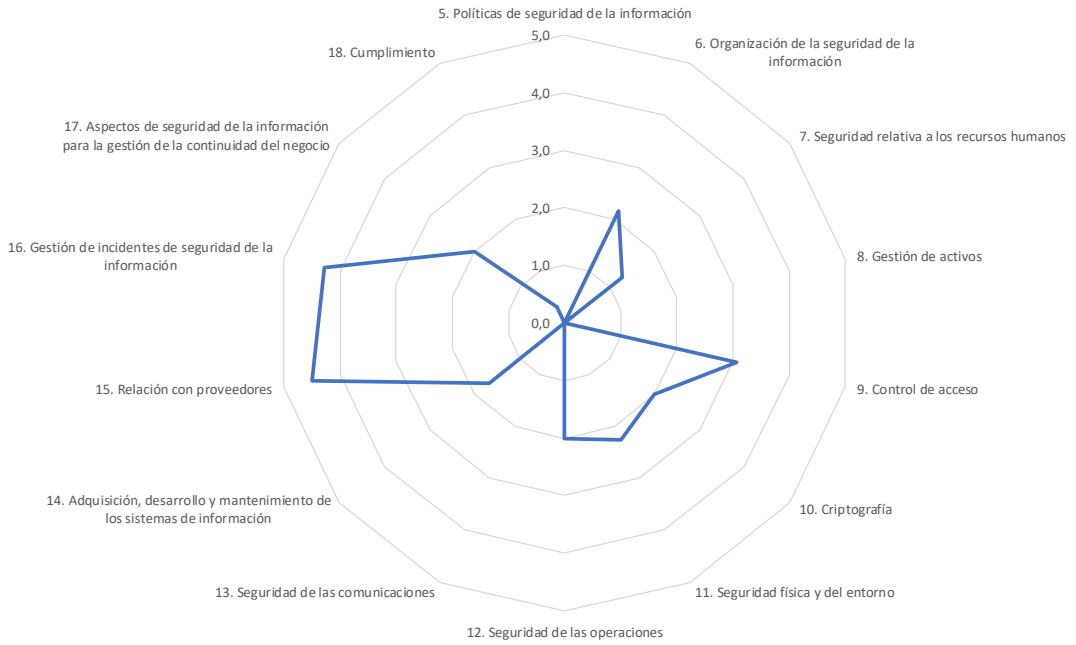


Imagen 8: Grado de madurez de los dominios de la ISO/IEC 27002

Para la realización de la anterior representación gráfica se ha procedido a evaluar el grado de madurez, según CMM, de cada control. Con los valores de los diferentes controles, se ha obtenido el valor de cada categoría promediando los diferentes valores de los controles contenidos en ésta. A su vez con los valores de las diferentes categorías se ha obtenido el valor del correspondiente capítulo (valor representado) promediando los diferentes valores de las categorías contenidas en el capítulo.

Cabe destacar que muchos de los valores detallados en la anterior gráfica son ‘0’ por desconocerse el estado actual del control.

2. ESQUEMA DOCUMENTAL

En la ISO/IEC 27001:2013 se definen una serie de documentos a desarrollar para la implantación y control del SGSI. A pesar de que en la norma se enumeran gran cantidad de documentos, no todos ellos son requeridos para la obtención de la certificación ISO/IEC 27001:2013.

A continuación, se detallan los documentos definidos como esquema documental básico del presente SGSI. A título informativo se indica en qué punto de la norma se hace referencia a dicho documento.

Documento	**Capítulo de ISO/IEC 27001:2013**
Políticas de Seguridad de la Información	5.2, 6.2
Procedimiento de Auditorías	9.2
Gestión de Indicadores	9.1
Procedimiento de Revisión por parte de la Dirección	9.3
Gestión de Roles y Responsabilidades	A.7.1.2
Metodología de Análisis de Riesgos	6.1.2 6.1.3 e), 6.2
Declaración de Aplicabilidad (SoA)	6.1.3 d)

Tabla 3: Esquema documental en base a la ISO/IEC 27001:2013

Lo primero que hará un auditor será revisar toda la documentación que existe en el SGSI y pedir evidencias de los documentos que son requeridos por la norma. Parte de esta documentación será la detallada en el listado anterior.

A continuación se resume brevemente el contenido de cada uno de los anteriores documentos así como el nombre exacto del fichero que recoge cada uno éstos.

2.1 Políticas de Seguridad de la Información

Recoge las Políticas de Seguridad de la Información que son de aplicación a los procesos seguidos por las Áreas Comercial y de Operaciones relativos a la gestión de la información relacionada con oportunidades de negocio, o preventas, y/o la ejecución de proyectos.

El objetivo de las Políticas de Seguridad de la Información definidas en el presente documento es el de proteger los activos de información de Integrador X de amenazas internas, externas, intencionadas o accidentales, minimizando el riesgo a través de la prevención de incidentes y la reducción de su impacto potencial.

MuñozMercaderEDGAR_TFM_Politica_Seguridad de la Informacion v1.1.pdf

2.2 Procedimiento de Auditorías

Detalla el Plan de Auditorías a ejecutar al amparo del SGSI.

La organización debe llevar a cabo las auditorías internas a intervalos planificados, para proporcionar información sobre el SGSI:

- Está conforme con los requisitos de la empresa para su sistema de gestión y los requisitos de la norma ISO/IEC 27001
- Está implementado y mantenido de forma eficaz

MuñozMercaderEDGAR_TFM_Procedimiento de Auditorias v1.1.pdf

2.3 Gestión de Indicadores

Detalla la Gestión de Indicadores a desarrollar al amparo del SGSI con los que se debe evaluar el desempeño de la Seguridad de la Información y la eficacia del SGSI.

MuñozMercaderEDGAR_TFM_Gestion de Indicadores v1.1.pdf

2.4 Procedimiento de Revisión por parte de la Dirección

Detalla el procedimiento a través del cual la Dirección de Integrador X revisa el SGSI.

En el ámbito de un SGSI, la Dirección de la organización juega un papel vital en su correcto desarrollo. La Dirección de Integrador X debe hacer revisiones periódicas del SGSI, analizando sus *outputs* y tomando las decisiones oportunas para la mejora continua y cualquier otra necesidad de cambio dentro del SGSI.

MuñozMercaderEDGAR_TFM_Procedimiento Revision por Direccion v1.1.pdf

2.5 Gestión de Roles y Responsabilidades

Detalla los diferentes Roles y Responsabilidades en el ámbito del SGSI. Define unívocamente los diferentes Roles y Responsabilidades para con las Políticas de Seguridad de la Información, cuyo principal objetivo es el de proteger los activos de información de Integrador X de amenazas internas, externas, intencionadas o accidentales, minimizando el riesgo a través de la prevención de incidentes y la reducción de su impacto potencial.

MuñozMercaderEDGAR_TFM_Roles y Responsabilidades v1.1.pdf

2.6 Metodología de Análisis de Riesgos

Detalla la metodología a utilizar para el Análisis de Riesgos a implementar al amparo del SGSI según la planificación definida.

MuñozMercaderEDGAR_TFM_Metodologia Analisis de Riesgos v1.1.pdf

2.7 Declaración de Aplicabilidad (SoA)

Proporciona la estructura de documento de Declaración de Aplicabilidad de los diferentes controles definidos en el Anexo A de la ISO/IEC 27001 en el SGSI.

La Declaración de Aplicabilidad (SoA, *Statement of Applicability*) es un requisito del estándar ISO/IEC 27001. Aunque no sea objetivo la obtención de dicha certificación, puede ser utilizado por cualquier organización como una manera de mantener el registro y control de las medidas de seguridad que son aplicadas al amparo de un SGSI.

MuñozMercaderEDGAR_TFM_Declaracion de Aplicabilidad v1.1.pdf

3. ANÁLISIS DE RIESGOS

Toda organización debe llevar a cabo valoraciones de riesgos de la Seguridad de la Información. Integrador X establece la metodología propuesta en el documento anexo al SGSI “MuñozMercaderEDGAR_TFM-_Metodologia Analisis de Riesgos v1.1.pdf” para llevar a cabo los Análisis de Riesgos correspondientes. Dicha metodología toma como referencia la metodología MAGERIT en su versión 3.

A grandes rasgos, las fases del análisis de riesgos definido en el ámbito del SGSI son:

- Identificación de Activos así como su valoración y dimensiones de seguridad
- Identificación de las Amenazas que pueden afectar a estos activos
- Cálculo del posible Impacto que dichas amenazas pueden representar sobre los Activos
- Cálculo del Riesgo al que está expuesta la organización.

En función del Riesgo Aceptable definido por Integrador X en sus Políticas de Seguridad de la Información, detalladas en el documento anexo “MuñozMercaderEDGAR_TFM_Politica_Seguridad de la Informacion v1.1.pdf”, se deberá aplicar salvaguardas / contramedidas / controles para mitigar aquellos riesgos que superen dicho umbral.

Después de aplicar estos controles, el riesgo que permanece -idealmente por debajo del Riesgo Aceptable por la organización- es el Riesgo Residual.

A continuación se detalla el Análisis de Riesgos realizado en Integrador X en el ámbito del presente SGSI.

3.1 Identificación de Activos

Como primer paso, y siguiendo la metodología definida, se debe realizar una Identificación de Activos.

En primera instancia se identifican los **Activos Esenciales** que marcarán los requisitos de la Seguridad de la Información del SGSI. En el ámbito del SGSI, definido en el punto 1.2.3, podemos definir tres activos esenciales:

- **[S] Servicios de Ejecución de Proyectos**
- **[I] Información relativa a Oportunidades de Negocio / Operaciones de Preventa**
- **[I] Información relativa a la Ejecución de Proyecto**

Subordinados a estos activos encontramos otros activos de soporte o secundarios. A continuación se muestran estos activos agrupados según las categorías enunciadas en la metodología de Análisis de Riesgos definida para el SGSI.

- Instalaciones
  - [L] CPD
  - [L] Oficina
- Hardware

- [HW] Cabinas de discos
- [HW] Dispositivos móviles (smartphones o tablets)
- [HW] Proxy de navegación
- [HW] Puestos de trabajo (desktops o laptops)
- [HW] Servidores en CPD
- [HW] Sistemas de impresión

- Aplicaciones
  - [SW] Antivirus/antimalware
  - [SW] Aplicaciones a medida de Gestión de Proyectos
  - [SW] Aplicaciones ofimáticas
  - [SW] Aplicación de backup
  - [SW] Desarrollos propios

- Datos
  - [D] Código fuente
  - [D] Documentos ofimáticos

- Redes de Comunicaciones
  - [COM] Acceso a Internet
  - [COM] Comunicaciones LAN/WAN (electrónica de red, routers, firewalls, etc.)

- Servicios Auxiliares
  - [SS] Servicios en formato SaaS (Software as a Service): correo, MI, directorio, storage
  - [SS] Servidores en formato IaaS (Infrastructure as a Service)

- Equipamiento Auxiliar
  - [Media] CD-Rom, DVD, Memoria USB
  - [Media] Documentación en formato papel
  - [AUX] Destructora de documentos
  - [AUX] Sistema de cableado
  - [AUX] UPS, Generadores eléctricos, Equipo de clima, etc.

- Personal
  - [P] Administrador de comunicaciones
  - [P] Administrador de seguridad
  - [P] Administrador de sistemas
  - [P] Usuarios

Viendo las diferentes categorías de los activos identificados se establece una jerarquía entre éstas tal y como se muestra a continuación.

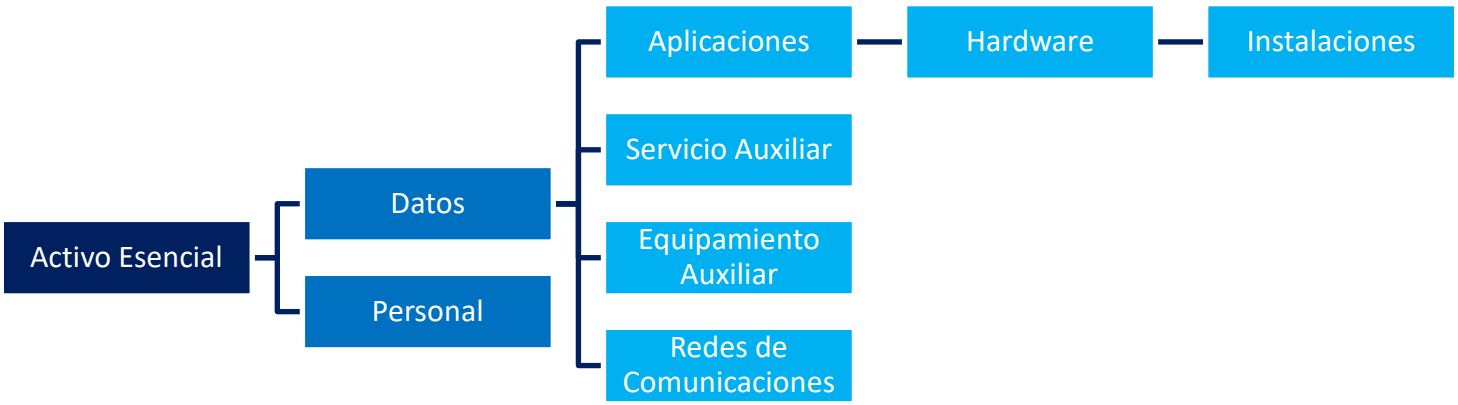


Imagen 9: Jerarquía entre activos

En base a la anterior información: activos identificados y categorizados y la jerarquía de categorías definida, es posible construir la siguiente tabla donde se relaciona cada activo con su categoría y con la categoría inmediatamente superior que complementa. Esta tabla se será útil a la hora de considerar como riesgos de activos de categorías inferiores tienen repercusión sobre los riesgos de activos de las categorías que conforman (categorías superiores).

Categoría	**Activo**	**Categoría superior**
Activos Esenciales	[S] Servicios de Ejecución de Proyectos	-
Activos Esenciales	[I] Información relativa a Oportunidades de Negocio / Operaciones de Preventa	-
Activos Esenciales	[I] Información relativa a la Ejecución de Proyecto	-
Instalaciones	[L] CPD	Hardware
Instalaciones	[L] Oficina	Hardware

Categoría	**Activo**	**Categoría superior**
Hardware	[HW] Cabinas de discos	Aplicaciones
Hardware	[HW] Dispositivos móviles (smartphones o tablets)	Aplicaciones
Hardware	[HW] Proxy de navegación	Aplicaciones
Hardware	[HW] Puestos de trabajo (desktops o laptops)	Aplicaciones
Hardware	[HW] Servidores en CPD	Aplicaciones
Hardware	[HW] Sistemas de impresión	Aplicaciones
Aplicaciones	[SW] Antivirus/antimalware	Datos
Aplicaciones	[SW] Aplicaciones a medida de Gestión de Proyectos	Datos
Aplicaciones	[SW] Aplicaciones ofimáticas	Datos
Aplicaciones	[SW] Aplicación de backup	Datos
Aplicaciones	[SW] Desarrollos propios	Datos
Datos	[D] Código fuente	**Activos Esenciales**
Datos	[D] Documentos ofimáticos	**Activos Esenciales**
Redes de Comunicaciones	[COM] Acceso a Internet	Datos
Redes de Comunicaciones	[COM] Comunicaciones LAN/WAN (electrónica de red, routers, firewalls, etc.)	Datos
Servicios Auxiliares	[SS] Servicios en formato SaaS (Software as a Service): correo, MI, directorio, storage	Datos
Servicios Auxiliares	[SS] Servidores en formato IaaS (Infrastructure as a Service)	Datos
Equipamiento Auxiliar	[Media] CD-Rom, DVD, Memoria USB	Datos

Categoría	**Activo**	**Categoría superior**
Equipamiento Auxiliar	[Media] Documentación en formato papel	Datos
Equipamiento Auxiliar	[AUX] Destructora de documentos	Datos
Equipamiento Auxiliar	[AUX] Sistema de cableado	Datos
Equipamiento Auxiliar	[AUX] UPS, Generadores eléctricos, Equipo de clima, etc.	Datos
Personal	[P] Administrador de comunicaciones	**Activos Esenciales**
Personal	[P] Administrador de seguridad	**Activos Esenciales**
Personal	[P] Administrador de sistemas	**Activos Esenciales**
Personal	[P] Usuarios	**Activos Esenciales**

Tabla 4: Relación de activos categorizados y categoría superior

3.1.1 Valoración de Activos

Una vez identificados y categorizados los diferentes activos (Tabla 4) se procede a realizar su valoración en base a los siguientes valores:

- MA: Muy Alto
- A. Alto
- M: Medio
- B: Bajo
- MB: Muy Bajo

Es necesario hacer hincapié que para la definición del valor de los activos se debe considerar cual sería el daño que supondría para la organización su perdida, alteración o filtración de dichos activos y no en base a su valor material o valor que costaría reponer ese activo. La valoración de los activos debe ser vista desde el punto de vista de la “necesidad de proteger” esos activos de las amenazas a los que están expuestos.

Con todo lo anterior se procede a incorporar a la Tabla 4 la valoración de los diferentes activos:

Categoría	**Activo**	**Categoría superior**	**Valor**
Activos Esenciales	[S] Servicios de Ejecución de Proyectos	-	A
Activos Esenciales	[I] Información relativa a Oportunidades de Negocio / Operaciones de Preventa	-	MA
Activos Esenciales	[I] Información relativa a la Ejecución de Proyecto	-	MA
Instalaciones	[L] CPD	Hardware	A
Instalaciones	[L] Oficina	Hardware	MB
Hardware	[HW] Cabinas de discos	Aplicaciones	A
Hardware	[HW] Dispositivos móviles (smartphones o tablets)	Aplicaciones	B
Hardware	[HW] Proxy de navegación	Aplicaciones	B
Hardware	[HW] Puestos de trabajo (desktops o laptops)	Aplicaciones	M
Hardware	[HW] Servidores en CPD	Aplicaciones	A
Hardware	[HW] Sistemas de impresión	Aplicaciones	MB
Aplicaciones	[SW] Antivirus/antimalware	Datos	M
Aplicaciones	[SW] Aplicaciones a medida de Gestión de Proyectos	Datos	M
Aplicaciones	[SW] Aplicaciones ofimáticas	Datos	B
Aplicaciones	[SW] Aplicación de backup	Datos	M
Aplicaciones	[SW] Desarrollos propios	Datos	A
Datos	[D] Código fuente	**Activos Esenciales**	A
Datos	[D] Documentos ofimáticos	**Activos Esenciales**	A
Redes de Comunicaciones	[COM] Acceso a Internet	Datos	M

Categoría	Activo	Categoría superior	Valor
Redes de Comunicaciones	[COM] Comunicaciones LAN/WAN (electrónica de red, routers, firewalls, etc.)	Datos	B
Servicios Auxiliares	[SS] Servicios en formato SaaS (Software as a Service): correo, MI, directorio, storage	Datos	M
Servicios Auxiliares	[SS] Servidores en formato IaaS (Infrastructure as a Service)	Datos	B
Equipamiento Auxiliar	[Media] CD-Rom, DVD, Memoria USB	Datos	MB
Equipamiento Auxiliar	[Media] Documentación en formato papel	Datos	MB
Equipamiento Auxiliar	[AUX] Destructora de documentos	Datos	MB
Equipamiento Auxiliar	[AUX] Sistema de cableado	Datos	MB
Equipamiento Auxiliar	[AUX] UPS, Generadores eléctricos, Equipo de clima, etc.	Datos	MB
Personal	[P] Administrador de comunicaciones	**Activos Esenciales**	B
Personal	[P] Administrador de seguridad	**Activos Esenciales**	B
Personal	[P] Administrador de sistemas	**Activos Esenciales**	B
Personal	[P] Usuarios	**Activos Esenciales**	B

Tabla 5: Relación de activos valorados

3.1.2 Dimensiones de Seguridad de los activos

A continuación, para cada uno de los activos se definirán las diferentes dimensiones de seguridad y su valoración. Las dimensiones de seguridad a utilizar son las definidas en la metodología correspondiente -recogida en el documento "MuñozMercaderEDGAR_TFM_-Metodologia Analisis de Riesgos v1.1.pdf":

- **Autenticidad:** ¿Qué perjuicio causaría el no saber exactamente quién hace qué?

- **Confidencialidad:** ¿Qué daño causaría qué la información fuera conocida por quien no debe conocerla?
- **Integridad:** ¿Qué perjuicio causaría que la información fuera alterada?
- **Disponibilidad:** ¿Qué perjuicio causaría no poder disponer de la información / el servicio?
- **Trazabilidad:** ¿Qué daño causaría no saber a quién se le presta el servicio o quién accede a qué dato y qué hace con él?

La valoración de las dimensiones se cuantificará para cada activo y para cada dimensión en base a los criterios reflejados en la siguiente tabla, definidos la metodología de Análisis de Riesgos definida en el correspondiente documento anexo.

Valor	Criterio
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Sin daño o irrelevante para la organización

Tabla 6: Criterios de valoración de las dimensiones de seguridad de los activos

Este dato será incorporado a la tabla definida en el punto anterior (Tabla 5) quedando la tabla de la siguiente manera[3]:

Categoría	Activo	Categoría superior	Valor	Dimensiones				
				A	C	I	D	T
Activos Esenciales	[S] Servicios de Ejecución de Proyectos	-	A	1	7	5	6	1
Activos Esenciales	[I] Información relativa a Oportunidades de Negocio / Operaciones de Preventa	-	MA	1	7		4	
Activos Esenciales	[I] Información relativa a la Ejecución de Proyecto	-	MA	2	9		4	
Instalaciones	[L] CPD	Hardware	A				8	
Instalaciones	[L] Oficina	Hardware	MB				3	

[3] Las dimensiones de un activo concreto que no sean de aplicación desde el punto de vista de seguridad no serán informadas utilizando a todos los efectos un '0' en la valoración de la dimensión.

Categoría	Activo	Categoría superior	Valor	Dimensiones				
				A	C	I	D	T
Hardware	[HW] Cabinas de discos	Aplicaciones	A	7	6	7	6	5
Hardware	[HW] Dispositivos móviles (smartphones o tablets)	Aplicaciones	B		6	3	1	
Hardware	[HW] Proxy de navegación	Aplicaciones	B				3	
Hardware	[HW] Puestos de trabajo (desktops o laptops)	Aplicaciones	M		7	5	2	
Hardware	[HW] Servidores en CPD	Aplicaciones	A	7	6	6	6	5
Hardware	[HW] Sistemas de impresión	Aplicaciones	MB				1	
Aplicaciones	[SW] Antivirus/antimalware	Datos	M				4	
Aplicaciones	[SW] Aplicaciones a medida de Gestión de Proyectos	Datos	M		5	5	3	
Aplicaciones	[SW] Aplicaciones ofimáticas	Datos	B				4	
Aplicaciones	[SW] Aplicación de backup	Datos	M		6	8	5	
Aplicaciones	[SW] Desarrollos propios	Datos	A		7	5	5	
Datos	[D] Código fuente	**Activos Esenciales**	A	6	7	4	3	5
Datos	[D] Documentos ofimáticos	**Activos Esenciales**	A	7	7	4	3	4
Redes de Comunicaciones	[COM] Acceso a Internet	Datos	M		7	2	4	
Redes de Comunicaciones	[COM] Comunicaciones LAN/WAN (electrónica de red, routers, firewalls, etc.)	Datos	B		5	5	4	
Servicios Auxiliares	[SS] Servicios en formato SaaS (Software as a	Datos	M		6	6	7	

Categoría	Activo	Categoría superior	Valor	Dimensiones				
				A	C	I	D	T
	Service): correo, MI, directorio, storage							
Servicios Auxiliares	[SS] Servidores en formato IaaS (Infrastructure as a Service)	Datos	B	7	6	6	6	5
Equipamiento Auxiliar	[Media] CD-Rom, DVD, Memoria USB	Datos	MB		8	2		
Equipamiento Auxiliar	[Media] Documentación en formato papel	Datos	MB		4		2	
Equipamiento Auxiliar	[AUX] Destructora de documentos	Datos	MB				2	
Equipamiento Auxiliar	[AUX] Sistema de cableado	Datos	MB				1	
Equipamiento Auxiliar	[AUX] UPS, Generadores eléctricos, Equipo de clima, etc.	Datos	MB				4	
Personal	[P] Administrador de comunicaciones	**Activos Esenciales**	B				2	
Personal	[P] Administrador de seguridad	**Activos Esenciales**	B				3	
Personal	[P] Administrador de sistemas	**Activos Esenciales**	B				2	
Personal	[P] Usuarios	**Activos Esenciales**	B				2	

Tabla 7: Relación de activos con sus dimensiones de seguridad valoradas

3.2 Amenazas

A continuación se procede a identificar las posibles amenazas que potencialmente pueden causar un incidente que cause daños en los SI de Integrador X.

Para cada categoría de activo y para cada amenaza se establecerá una probabilidad de ocurrencia y la afectación de la amenaza sobre el activo. A la hora de indicar esta probabilidad y la afectación sobre el activo se han tenido en cuenta las actuales salvaguardas que en la actualidad Integrador X dispone.

A la hora de realizar la estimación de la probabilidad de ocurrencia de una amenaza se ha utilizado como patrón de unidad de medida los días en un año en que es factible que esa amenaza se materialice: por ejemplo, si es posible que una amenaza se materialice 1 día a lo largo de todo un año, su probabilidad será de 1/365, es decir de un 0,27%. A pesar de que 0,27% pueda parecer un valor bajo, se deberá relativizar las probabilidades obtenidas para todas las amenazas. Por el hecho de haber usado un patrón común, esta relativización es posible.

La afectación de una amenaza sobre un activo puede ser diferente para cada una de las dimensiones de seguridad. Por tanto, consideraremos las diferentes dimensiones de éstos estableciendo la afectación sobre cada una de ellas ante la ocurrencia de cada amenaza. Al igual que en la determinación de la probabilidad de ocurrencia de las amenazas, a la hora de determinar la afectación de una amenaza sobre sus diferentes dimensiones se han tenido en cuenta las actuales salvaguardas que Integrador X dispone en la actualidad.

Como se observará en los listados de amenazas mostrados a continuación, existen amenazas que afectan a diferentes categorías de activos. En estos casos, es posible que la probabilidad de ocurrencia y/o la afectación de una misma amenaza a diferentes categorías de activos sea diferente. Por ejemplo, no tendrá la misma afectación la materialización de la amenaza “[A.11] Acceso no autorizado” sobre un servidor (Hardware) que sobre un pendrive USB (Equipamiento Auxiliar).

Tal y como se indica en la metodología anexa en el documento “MuñozMercaderEDGAR-_TFM_Metodologia Analisis de Riesgos v1.1”, se utilizarán las amenazas definidas en la metodología MAGERIT. MAGERIT define 4 tipologías de amenazas:

- desastres naturales [N]
- de origen industrial [I]
- errores y fallos no intencionados [E]
- y ataques intencionados [A]

A continuación se detallan para la categoría de activo “Instalaciones” las amenazas identificadas con su correspondiente probabilidad de ocurrencia y afectación para cada una de las dimensiones. Se detallan las amenazas para todas las categorías de activos identificados en el anexo 6.1.

Amenaza	**Probabilidad (días/año)**	**Probabilidad**	**Degradación**				
			A	**C**	**I**	**D**	**T**
Instalaciones							
[N.1] Fuego	0,05	0,01%				20%	
[N.2] Daños por agua	0	0,00%				5%	
[N.*] Desastres naturales	0,01	0,00%				80%	
[I.1] Fuego	0,1	0,03%				20%	
[I.2] Daños por agua	1	0,27%				5%	
[I.*] Desastres industriales	1	0,27%				0%	

Amenaza	Probabilidad (días/año)	Probabilidad	Degradación				
			A	C	I	D	T
[I.11] Emanaciones electromagnéticas	0	0,01%		80%			
[E.15] Alteración accidental de la información	5	1,37%			1%		
[E.18] Destrucción de información	5	1,37%				1%	
E.19] Fugas de información	5	1,37%		1%			
[A.7] Uso no previsto	100	27,40%		0%	0%	0%	
[A.11] Acceso no autorizado	10	2,74%		1%	1%		
[A.15] Modificación deliberada de la información	0,1	0,03%			50%		
[A.18] Destrucción de información	0,1	0,03%				1%	
[A.19] Divulgación de información	1	0,27%		50%			
[A.26] Ataque destructivo	0,03	0,01%				20%	
[A.27] Ocupación enemiga	0	0,00%		50%		50%	

Tabla 8: Amenazas identificadas para la categoría de activo Instalaciones

3.3 Impacto

Una vez que la disponemos de los activos y amenazas identificadas y cuantificados sus principales parámetros:

- Activos: valor para Integrador X y la valoración de cada una de sus dimensiones
- Amenazas: probabilidad de ocurrencia y degradación sobre cada una de sus dimensiones

el procedimiento para la obtención del impacto es directo cruzando esta información.

A continuación, a modo de ejemplo, se procede a detallar el impacto que tendría la materialización de una amenaza de tipo “[E.2] Errores del administrador” sobre un activo “[HW] Cabinas de discos”.

A continuación se recuerdan las fichas del correspondientes al activo -extraída del punto 3.1.2- y a la amenaza -extraída del anexo 6.1 referenciado en el punto 3.2- con su correspondiente cuantificación.

Categoría	Activo	Categoría superior	Valor	Dimensiones				
				A	C	I	D	T
Hardware	[HW] Cabinas de discos	Aplicaciones	A	7	6	7	6	5

Tabla 9: Activo cuantificado

Amenaza	Probabilidad (días/año)	Probabilidad	Degradación				
			A	C	I	D	T
Hardware							
[E.2] Errores del administrador	4,00	1,10%		20%	20%	20%	

Tabla 10: Una de las amenazas asociada al activo de la Tabla 9

En el ejemplo escogido, la degradación sobre cada una de las dimensiones coincide para las dimensiones Confidencialidad, Integridad y Disponibilidad, pero no deja de ser una coincidencia que no tiene por qué darse en otros casos. Por ejemplo en las dimensiones Autenticidad y Trazabilidad la degradación no existe, es 0%.

Con la esta información, en primera instancia se calculará el impacto sobre el activo para cada una de sus dimensiones. Para ello, procederemos a aplicar el nivel de degradación sobre cada dimensión que implicaría la materialización de la amenaza sobre el activo.

Impacto				
A	C	I	D	T
7 x 0%	6 x 20%	7 x 20%	6 x 20%	5 x 0%

Impacto				
A	C	I	D	T
0,00	1,20	1,40	1,20	0,00

Tabla 11: Cálculo del Impacto

Como podemos observar en las tablas anteriores, el impacto es diferente para cada una de las dimensiones:

- Autenticidad: 0 impacto
- Confidencialidad: impacto de 1,2
- Integridad: impacto de 1,4
- Disponibilidad: impacto de 1,2
- Trazabilidad: 0 impacto

Por no añadir complejidad al análisis, asumiremos que el impacto "global" ante la materialización de una amenaza sobre un activo será el máximo de los impactos individuales de cada una de las dimensiones.

Impacto						Impacto
A	**C**	**I**	**D**	**T**		
0,00	1,20	1,40	1,20	0,00	=	Max (0,00, 1,20, 1,40, 1,20, 0,00) = 1,4

Tabla 12: Cálculo del Impacto del activo

Siguiendo el anterior proceso, se procede a calcular el impacto que producirían las diferentes amenazas al materializarse sobre los diferentes activos obteniendo un total de 593 indicadores de impacto, uno para cada pareja activo-amenaza.

Se muestra en el anexo 6.2 las tablas completas de los impactos calculados

3.4 Riesgo

Una vez calculados los impactos de las diferentes amenazas sobre los diferentes activos se está en disposición de determinar el riesgo al que está expuesto un activo a una amenaza. Este riesgo se determina en base a los impactos, calculados en el punto anterior, y a la probabilidad de materialización de cada amenaza, determinada en el punto 3.2.

Es habitual representar gráficamente los riesgos de cada activo-amenaza en base a su impacto en el eje de ordenadas (y) y la probabilidad de materialización de la amenaza en el eje de abscisas (x). Esta representación dará una visión muy gráfica del estado de riesgo asociado a los activos analizados.

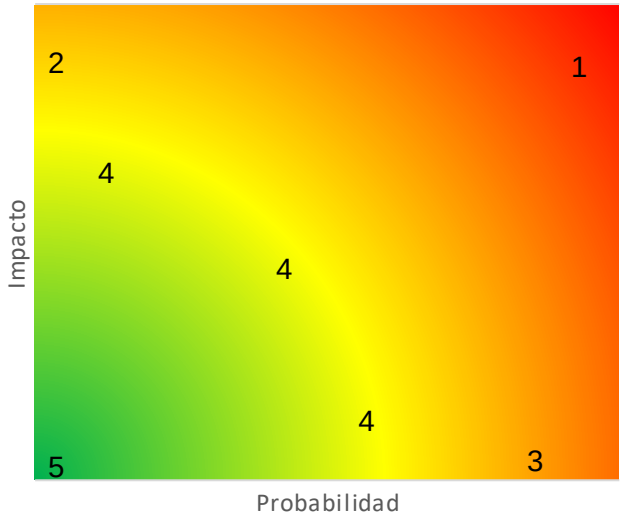


Imagen 10: Representación típica de Riesgos (Impacto/Probabilidad). Zonas de riesgo

Viendo el anterior diagrama se pueden observar, principalmente, 5 zonas de riesgo:

- Zona 1: riesgos muy probables y de alto impacto
- Zona 2: riesgos improbables pero de alto impacto

- Zona 3: riesgos muy probables pero de bajo impacto
- Zona 4: cubre una amplia casuística: riesgos improbables de impacto medio, riesgos probables de impacto bajo y otras casuísticas intermedias.
- Zona 5: riesgos improbables y de bajo impacto

En la siguiente gráfica se representan los riesgos determinados a lo largo de los anteriores apartados.

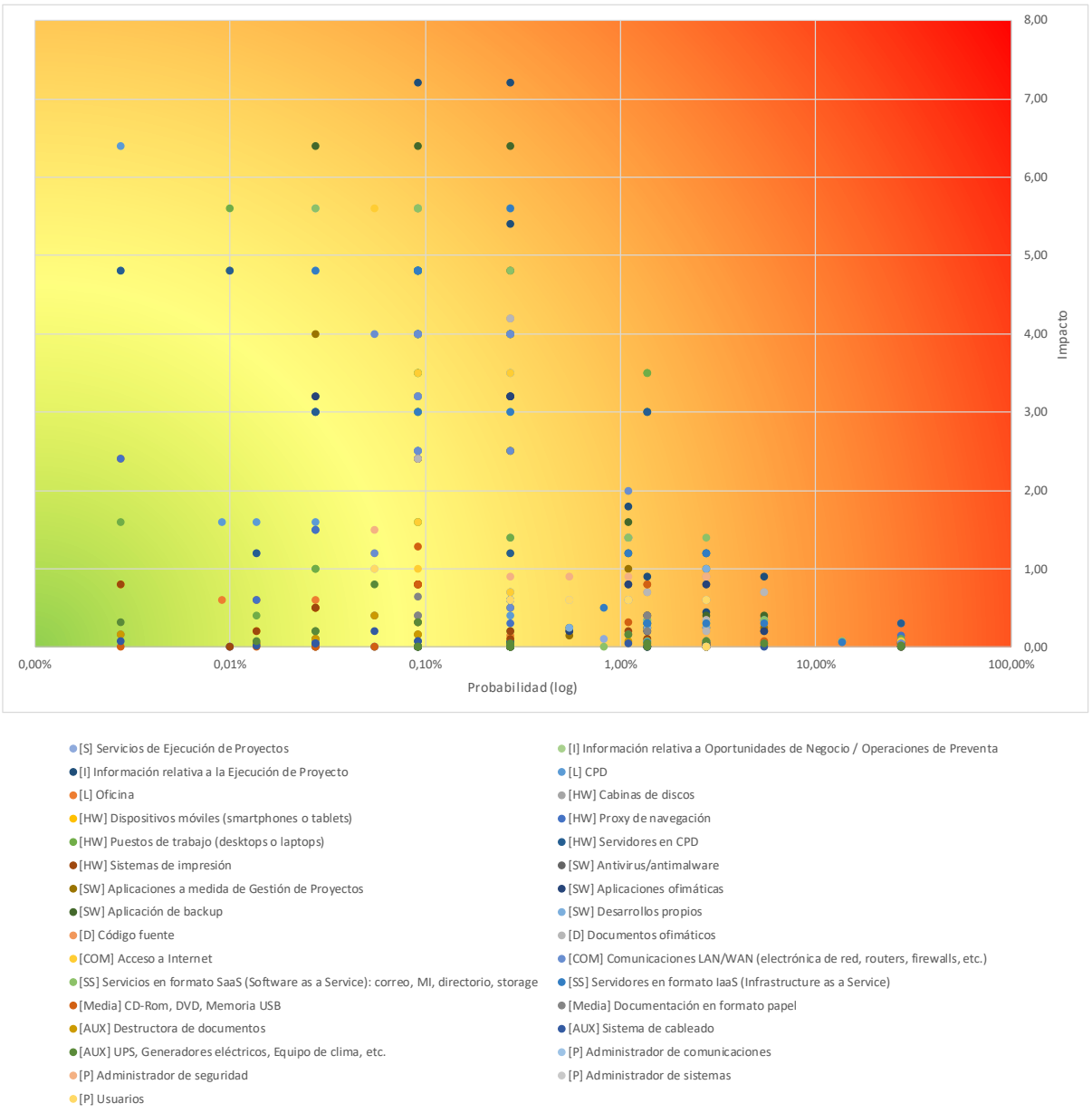


Imagen 11: Riesgos detectados

Nota: En la anterior representación se ha definido el eje de abscisas (y) en escala logarítmica para facilitar la lectura e interpretación de los datos.

Existe un tercer dato de relevancia -además del impacto y la probabilidad de ocurrencia- asociado al riesgo. Este dato, es el valor de cada uno de los activos para la organización. Este valor se define en el punto 3.1.1 y proporciona una idea de la necesidad de que cada activo sea protegido frente a las amenazas. Es posible incorporar este dato en la representación de la Imagen 9 definiendo el tamaño de los puntos en función del valor del activo. En la siguiente gráfica se incorpora dicha información.

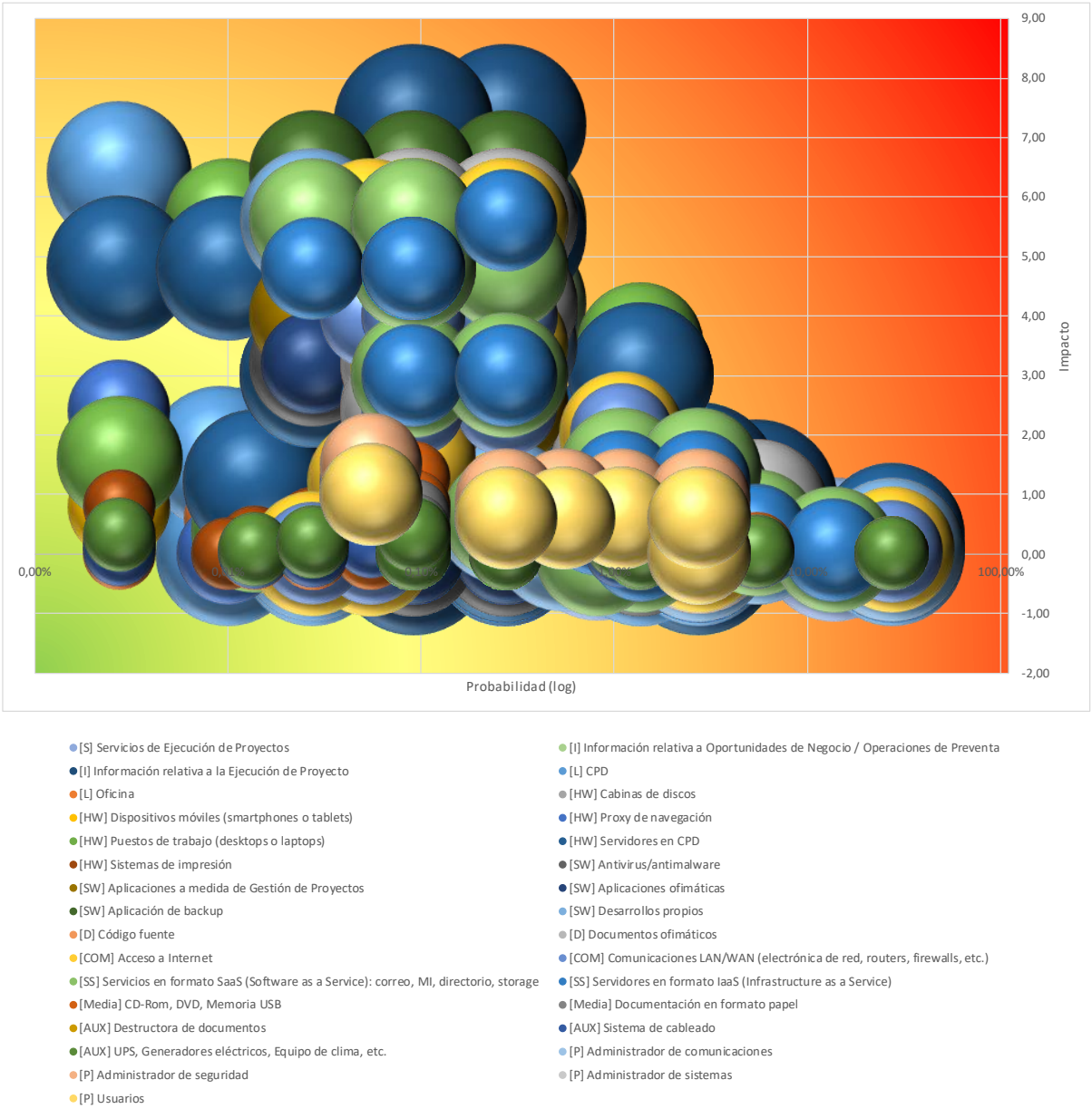


Imagen 12: Riesgos detectados ponderados por el valor del activo

Como puede observarse, se trata de una gráfica con gran cantidad de información. Con la intención de reducir la cantidad de información de la anterior gráfica, se anexa en el punto 6.3 las representaciones de riesgos (con la información del valor del activo) para cada una de las categorías de los activos definidos.

3.5 Conclusiones

Después de realizar el análisis de riesgos para el entorno del SGSI expuesto en los anteriores puntos a continuación se procede a analizar los resultados, extraer conclusiones y definir próximos pasos.

Es importante recordar que, en la definición de los activos, se estableció la dependencia entre las diferentes categorías de activos mostrada en la siguiente figura.

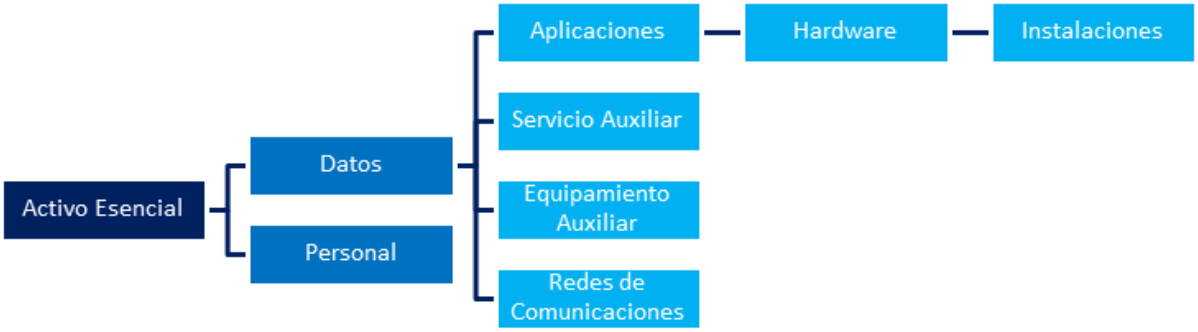


Imagen 13: Jerarquía entre activos

En el proceso de análisis de riesgos no se ha tenido en cuenta esta dependencia por no añadir complejidad adicional al análisis. Independientemente, analizando las dependencias mostradas en el anterior esquema se observa que un riesgo alto en cualquiera de los activos secundarios tendrá una repercusión sobre los Activos Esenciales y por tanto deberá de ser tratado.

Viendo la disposición de los riesgos determinados y el riesgo aceptable definido por la organización para el presente SGSI[4], se determina que los riesgos que superan el riesgo aceptado son los marcados en la siguiente gráfica mediante el recuadro azul[5].

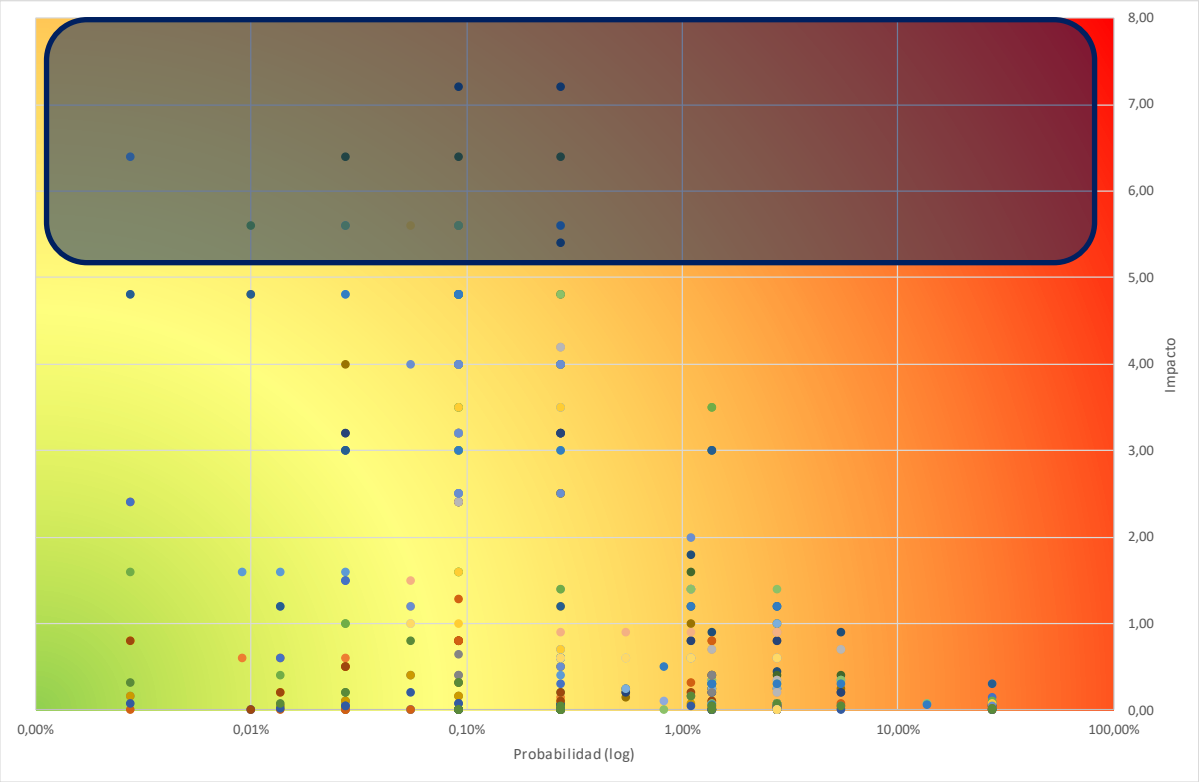


Imagen 14: Riesgos detectados

Estos riesgos son los correspondientes a:

Id Riesgo	Activo	Amenaza	Probabilidad	Impacto
1	[I] Información relativa a la Ejecución de Proyecto	[A.5] Suplantación de la identidad del usuario	0,27%	7,20
2	[I] Información relativa a la Ejecución de Proyecto	[A.19] Divulgación de información	0,09%	7,20
3	[SW] Aplicación de backup	[E.8] Difusión de software dañino	0,27%	6,40
4	[SW] Aplicación de backup	[A.15] Modificación deliberada de la información	0,09%	6,40

[4] Según se define en las "Políticas de Seguridad de la Información" definidas en el documento anexo "MuñozMercaderEDGAR_TFM_Politica_Seguridad de la Informacion v1.1.pdf": "…Estos controles serán aplicados a aquellos riesgos identificados cuyo impacto sea alto, con independencia de la probabilidad de ocurrencia, -zonas 1 y 2 según Metodología de Análisis de Riesgos…". Por tanto el riesgo aceptable definido por la organización para el presente SGSI son aquellos que no se encuentren en las zonas 1 o 2.

[5] Como se verá a continuación, no todos los riesgos se ven en la gráfica debido a que éstos se solapan y en estos casos el software de representación gráfica sólo muestra el primero de ellos.

Id Riesgo	Activo	Amenaza	Probabilidad	Impacto
5	[SW] Aplicación de backup	[A.22] Manipulación de programas	0,03%	6,40
6	[L] CPD	[N.*] Desastres naturales	0,00%	6,40
7	[S] Servicios de Ejecución de Proyectos	[A.5] Suplantación de la identidad del usuario	0,27%	5,60
8	[I] Información relativa a Oportunidades de Negocio / Operaciones de Preventa	[A.5] Suplantación de la identidad del usuario	0,27%	5,60
9	[SW] Desarrollos propios	[E.8] Difusión de software dañino	0,27%	5,60
10	[SW] Desarrollos propios	[A.5] Suplantación de la identidad del usuario	0,27%	5,60
11	[D] Código fuente	[A.5] Suplantación de la identidad del usuario	0,27%	5,60
12	[D] Documentos ofimáticos	[A.5] Suplantación de la identidad del usuario	0,27%	5,60
13	[COM] Acceso a Internet	[I.8] Fallo de servicios de comunicaciones	0,27%	5,60
14	[COM] Acceso a Internet	[A.5] Suplantación de la identidad del usuario	0,27%	5,60
15	[SS] Servidores en formato IaaS (Infrastructure as a Service)	[A.5] Suplantación de la identidad del usuario	0,27%	5,60
16	[S] Servicios de Ejecución de Proyectos	[A.9] [Re-]encaminamiento de mensajes	0,09%	5,60
17	[S] Servicios de Ejecución de Proyectos	[A.19] Divulgación de información	0,09%	5,60
18	[I] Información relativa a Oportunidades de Negocio / Operaciones de Preventa	[A.19] Divulgación de información	0,09%	5,60
19	[SW] Desarrollos propios	[A.9] [Re-]encaminamiento de mensajes	0,09%	5,60
20	[SW] Desarrollos propios	[A.19] Divulgación de información	0,09%	5,60
21	[D] Código fuente	[A.19] Divulgación de información	0,09%	5,60
22	[D] Documentos ofimáticos	[A.19] Divulgación de información	0,09%	5,60
23	[COM] Acceso a Internet	[A.9] [Re-]encaminamiento de mensajes	0,09%	5,60
24	[COM] Acceso a Internet	[A.19] Divulgación de información	0,09%	5,60

Id Riesgo	Activo	Amenaza	Probabilidad	Impacto
25	[SS] Servicios en formato SaaS (Software as a Service): correo, MI, directorio, storage	[A.18] Destrucción de información	0,09%	5,60
26	[SS] Servicios en formato SaaS (Software as a Service): correo, MI, directorio, storage	[A.24] Denegación de servicio	0,09%	5,60
27	[COM] Acceso a Internet	[A.14] Interceptación de información (escucha)	0,05%	5,60
28	[SW] Desarrollos propios	[A.22] Manipulación de programas	0,03%	5,60
29	[SS] Servicios en formato SaaS (Software as a Service): correo, MI, directorio, storage	[E.24] Caída del sistema por agotamiento de recursos	0,03%	5,60
30	[HW] Puestos de trabajo (desktops o laptops)	[I.11] Emanaciones electromagnéticas	0,01%	5,60
31	[I] Información relativa a la Ejecución de Proyecto	[A.11] Acceso no autorizado	0,27%	5,40

Tabla 13: Riesgos que superan el umbral aceptado

Será por tanto para estos 31 riesgos que superan el riesgo aceptado por la compañía, para los que se deberán definir controles y contramedidas para ser mitigados y reducir el riesgo (riesgo residual[6]) por debajo del riesgo aceptable. En los próximos puntos del presente documento se procederá a definir estos controles y contramedidas.

[6] Es el riesgo que permanece una vez se han aplicado las medidas correctivas definidas.

4. PROYECTOS DE MEJORA DE SEGURIDAD DE LA INFORMACIÓN

En toda Gestión de Riesgos, habitualmente, las acciones a realizar en relación con los riesgos identificados pueden ser de tipo:

- Asunción: Aceptar el riesgo y continuar con la operativa habitual conociendo la situación de riesgo a la que se está expuesto.
- Evitación: Evitar el riesgo erradicando la causa y/o la consecuencia.
- Reducción: Implementar controles o salvaguardas que minimicen el impacto de una amenaza que explote una vulnerabilidad.
- Transferencia: Transferir el riesgo a un tercero.

En el presente apartado se procederá a la definición de las acciones a adoptar por parte de Integrador X para la gestión de los riesgos que superen el nivel aceptado por la compañía e identificados en la Tabla 13 del anterior punto.

Analizando los 31 riesgos -binomio formado por activo y amenaza- se extrae la siguiente información de utilidad a la hora de definir las acciones a tomar para su gestión:

- Los 31 riesgos tienen en común 14 amenazas:

[A.11] Acceso no autorizado
[A.14] Interceptación de información (escucha)
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.5] Suplantación de la identidad del usuario
[A.9] [Re-]encaminamiento de mensajes
[E.24] Caída del sistema por agotamiento de recursos
[E.8] Difusión de software dañino
[I.11] Emanaciones electromagnéticas
[I.8] Fallo de servicios de comunicaciones

[N.*] Desastres naturales

- y afecta a 12 activos:

[COM] Acceso a Internet
[D] Código fuente
[D] Documentos ofimáticos
[HW] Puestos de trabajo (desktops o laptops)
[I] Información relativa a la Ejecución de Proyecto
[I] Información relativa a Oportunidades de Negocio / Operaciones de Preventa
[L] CPD
[S] Servicios de Ejecución de Proyectos
[SS] Servicios en formato SaaS (Software as a Service): correo, MI, directorio, storage
[SS] Servidores en formato IaaS (Infrastructure as a Service)
[SW] Aplicación de backup
[SW] Desarrollos propios

Esta manera de presentar los 31 riesgos a gestionar -agrupados por amenazas y/o por activos afectados- permiten observar puntos en común entre ellos. Viendo estos puntos en común ayuda a la definición de las acciones de gestión a tomar de manera que se aprovechen sinergias entre las diferentes amenazas y/o activos.

A continuación se definen acciones para la gestión para los riegos identificados. En próximos apartados se procederá a desarrollar las fichas de las diferentes acciones propuestas.

Asunción:

No se definen acciones de asunción para los riesgos detectados: todos ellos superan el umbral establecido por la Políticas de Seguridad y, por tanto, es conveniente la definición de una u otra acción.

Evitación:

No se definen acciones de evitación por no ser de aplicación real para los riesgos detectados.

Reducción:

Se definen las siguientes acciones para la reducción de los siguientes riesgos:

- **Implementación de un sistema criptográfico corporativo de clave pública (PKI) acompañado de una solución de cifrado de la información y las comunicaciones**
  Impacto total de los riesgos de aplicación[7]: **92.6**

  Los riesgos sobre las que se pretende actuar con la implementación de esta acción son:
  - [A.11] Acceso no autorizado
    - [I] Información relativa a la Ejecución de Proyecto
  - [A.14] Interceptación de información (escucha)
    - [COM] Acceso a Internet
  - [A.15] Modificación deliberada de la información
    - [SW] Aplicación de backup
  - [A.19] Divulgación de información
    - [I] Información relativa a la Ejecución de Proyecto
    - [S] Servicios de Ejecución de Proyectos
    - [I] Información relativa a Oportunidades de Negocio / Operaciones de Preventa
    - [SW] Desarrollos propios
    - [D] Código fuente
    - [D] Documentos ofimáticos
    - [COM] Acceso a Internet
  - [A.22] Manipulación de programas
    - [SW] Aplicación de backup
    - [SW] Desarrollos propios
  - [A.9] [Re-]encaminamiento de mensajes
    - [S] Servicios de Ejecución de Proyectos
    - [SW] Desarrollos propios
    - [COM] Acceso a Internet
  - [I.11] Emanaciones electromagnéticas
    - [HW] Puestos de trabajo (desktops o laptops)

- **Implementación de un sistema de autenticación de doble factor**
  Impacto total de los riesgos de aplicación: **63.8**

  Los riesgos sobre las que se pretende actuar con la implementación de esta acción son:
  - [A.11] Acceso no autorizado
    - [I] Información relativa a la Ejecución de Proyecto
  - [A.5] Suplantación de la identidad del usuario
    - [I] Información relativa a la Ejecución de Proyecto
    - [S] Servicios de Ejecución de Proyectos
    - [I] Información relativa a Oportunidades de Negocio / Operaciones de Preventa

[7] Para cada acción propuesta se indica el "Impacto total de los riesgos de aplicación" siendo la suma de los impactos de los riesgos que se pretende afrontar con la implementación de cada medida (en el cómputo únicamente se contemplan los riesgos que superan el nivel de riesgo aceptado por la organización). Este indicador será utilizado como referencia de la importancia/urgencia de la acción propuesta.

  - [SW] Desarrollos propios
  - [D] Código fuente
  - [D] Documentos ofimáticos
  - [COM] Acceso a Internet
  - [SS] Servidores en formato IaaS (Infrastructure as a Service)
- [A.22] Manipulación de programas
  - [SW] Aplicación de backup
- [A.18] Destrucción de información
  - [SS] Servicios en formato SaaS (Software as a Service): correo, MI, directorio, storage

- **Implementación de un sistema DLP (Data Loss Prevention)**
  Impacto total de los riesgos de aplicación: **40.8**

  Los riesgos sobre las que se pretende actuar con la implementación de esta acción son:
  - [A.19] Divulgación de información
    - [I] Información relativa a la Ejecución de Proyecto
    - [S] Servicios de Ejecución de Proyectos
    - [I] Información relativa a Oportunidades de Negocio / Operaciones de Preventa
    - [SW] Desarrollos propios
    - [D] Código fuente
    - [D] Documentos ofimáticos
    - [COM] Acceso a Internet

- **Impartición de formación / concienciación en el ámbito de la Seguridad de la Información**
  Impacto total de los riesgos de aplicación: **40.8**

  Los riesgos sobre las que se pretende actuar con la implementación de esta acción son:
  - [A.19] Divulgación de información
    - [I] Información relativa a la Ejecución de Proyecto
    - [S] Servicios de Ejecución de Proyectos
    - [I] Información relativa a Oportunidades de Negocio / Operaciones de Preventa
    - [SW] Desarrollos propios
    - [D] Código fuente
    - [D] Documentos ofimáticos
    - [COM] Acceso a Internet

- **Implementación de un sistema de backup de la información en cloud**
  Impacto total de los riesgos de aplicación: **16.8**

  Los riesgos sobre las que se pretende actuar con la implementación de esta acción son:
  - [A.18] Destrucción de información
    - [SS] Servicios en formato SaaS (Software as a Service): correo, MI, directorio, storage
  - [A.24] Denegación de servicio
    - [SS] Servicios en formato SaaS (Software as a Service): correo, MI, directorio, storage
  - [E.24] Caída del sistema por agotamiento de recursos
    - [SS] Servicios en formato SaaS (Software as a Service): correo, MI, directorio, storage

- **Implantación de sistemas Antimalware, ZeroDay, anti-APT**

Impacto total de los riesgos de aplicación: **12**

Los riesgos sobre las que se pretende actuar con la implementación de esta acción son:

- [E.8] Difusión de software dañino
  - [SW] Aplicación de backup
  - [SW] Desarrollos propios

- **Contratación de los Servicios de un CPD de respaldo**
  Impacto total de los riesgos de aplicación: **6.4**

  Los riesgos sobre las que se pretende actuar con la implementación de esta acción son:
  - [N.*] Desastres naturales
    - [L] CPD

- **Implantación de un sistema de Anti-DDoS**
  Impacto total de los riesgos de aplicación: **5.6**

  Los riesgos sobre las que se pretende actuar con la implementación de esta acción son:
  - [A.24] Denegación de servicio
    - [SS] Servicios en formato SaaS (Software as a Service): correo, MI, directorio, storage

- **Implementación de redundancia / alta disponibilidad en las comunicaciones corporativas**
  Impacto total de los riesgos de aplicación: **5.6**

  Los riesgos sobre las que se pretende actuar con la implementación de esta acción son:
  - [I.8] Fallo de servicios de comunicaciones
    - [COM] Acceso a Internet

Transferencia:

- **Definición de ANS (o SLA) acordes con los requerimientos del negocio**
  Impacto total de los riesgos de aplicación: **11.2**

  Los riesgos sobre las que se pretende actuar con la implementación de esta acción son:
  - [A.24] Denegación de servicio
    - [SS] Servicios en formato SaaS (Software as a Service): correo, MI, directorio, storage
  - [E.24] Caída del sistema por agotamiento de recursos
    - [SS] Servicios en formato SaaS (Software as a Service): correo, MI, directorio, storage

- **Contratación de seguro con cobertura de los Desastres Naturales en el ámbito del CPD**
  Impacto total de los riesgos de aplicación: **6.4**

  Los riesgos sobre las que se pretende actuar con la implementación de esta acción son:
  - [N.*] Desastres naturales
    - [L] CPD

A continuación se procederá a proporcionar mayor detalle de los proyectos enumerados anteriormente proporcionando: una descripción de los mismos, una propuesta de controles que permitan medir la penetración y/o efectividad del proyecto, una duración y costes estimados de implantación, los recursos internos requeridos así como el departamento o dirección que debería asumir la responsabilidad para la implementación de cada uno de los proyectos propuestos.

Al respecto de la estimación de los costes, ésta se realizará en base a las siguientes horquillas económicas:

- Bajo: coste de implementación de 1.000 a 100.000 €
- Medio: coste de implementación de 100.001 a 700.000 €
- Alto: coste de implementación de más de 700.001 €

No es objeto de los próximos apartados definir en detalle los diferentes proyectos. Esta labor será realizada una vez se disponga de las correspondientes aprobaciones, asignación presupuestaria, etc. Llegado el caso deberá concretarse el alcance de los proyectos, opción escogida entre las diferentes alternativas, etc. que mejor se adapten a las necesidades y requerimientos de seguridad de Integrador X.

Por último, en el punto 4.12 se mostrará un resumen de la información relevante de las diferentes propuestas con el objetivo de facilitar la toma de decisión de que proyectos a abordar, su priorización y planificación.

4.1 Implementación de un sistema criptográfico corporativo de clave pública (PKI) acompañado de una solución de cifrado de la información y las comunicaciones

El objetivo del presente proyecto es la aplicación de controles que mitiguen el impacto y/o la probabilidad de ocurrencia de las amenazas:

- [A.11] Acceso no autorizado
- [A.14] Interceptación de información (escucha)
- [A.15] Modificación deliberada de la información
- [A.19] Divulgación de información
- [A.22] Manipulación de programas
- [A.9] [Re-]encaminamiento de mensajes
- [I.11] Emanaciones electromagnéticas

El impacto acumulado de los riesgos asociados a las anteriores amenazas es de 92.6.

Gestión de tipo Reducción del Riesgo.

Descripción del proyecto:

Un sistema criptográfico asimétrico (o de clave pública) consiste en la generación de un par de claves para cada individuo: clave pública y clave privada. La clave pública de cada persona es conocida por todo aquel que desee comunicar con éste, en cambio, la clave privada solo debe ser conocida por del usuario propietario de ésta.

Por definición, en un sistema de claves asimétrico la información cifrada con una clave pública sólo puede ser descifrada por su correspondiente clave privada y viceversa.

Esta característica permite a cualquier usuario enviar un mensaje a un destinatario concreto y que sólo éste pueda leer su contenido. Si el emisor cifra el contenido del mensaje con la clave pública del destinatario, sólo el destinatario legítimo podrá acceder a su contenido usando su clave privada.

Imagen 15: Cifrado de mensajes

Utilizando el mismo principio, si un usuario cifra un mensaje con su clave privada, cualquier usuario podrá acceder al contenido del mensaje utilizando su clave pública. De esta manera, se tiene la certeza de que el origen del mensaje es el usuario propietario de la correspondiente clave privada.

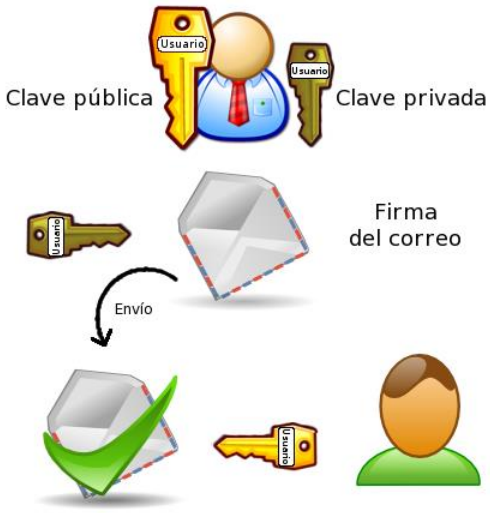


Imagen 16: Firma digital de mensajes

Los dos anteriores principios pueden ser combinados y enviar un mensaje cifrado para que sólo el destinatario legítimo puede leerlo con su clave privada a la vez que se puede firmar el

hash[8] del mensaje con la clave privada del emisor y así validar el emisor del mensaje mediante su clave pública.

Esta solución acompañada de un sistema que permita el cifrado de la información y de las comunicaciones permitirá dotar a los SI de Confidencialidad, Integridad, Autenticación y No Repudio.

El sistema a desplegar debe cumplir con los siguientes requerimientos:

- Debe permitir la emisión de certificados tanto a personas físicas como a sistemas de TI que puedan requerir de estas funcionalidades: servidores, routers, etc.
- Debe garantizar la inviolabilidad de las claves privadas generadas y almacenadas en el sistema.
- Debe hacer uso de algoritmos criptográficos seguros ampliamente aceptados por el sector.
- Debe permitir el cifrado de la información “en reposo” en sus correspondientes sistemas de almacenamiento (sistemas de ficheros, bases de datos, soportes de backup, etc.), como “en tránsito”.
- En todo caso que sea posible, la información sólo debe ser accesible “en claro” por el destinario legítimo de la información. En los casos de información compartida entre varios, ésta debe ser accesible, sólo por aquellas personas que deban tener acceso a su contenido.

Controles:

- % de usuarios / sistemas con certificado emitido
- % de información cifrada almacenada
- % de comunicaciones cifradas

Duración:

- 6 meses para la implantación de la infraestructura de PKI
- 3 meses para la implantación de las soluciones de cifrado
- 3 meses para el despliegue de la solución entre los usuarios

Coste:

- Medio

Recursos Necesarios:

- Consultor de Seguridad (30%)
- Recursos de Sistemas (por ejemplo, máquinas virtuales para albergar los diferentes roles del sistema).
- Administrador de Sistemas (10%[9])

[8] Una función criptográfica hash es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

[9] Se indica en forma de tanto porcentual la dedicación estimada de los recursos requeridos para la implementación de cada proyecto.

Responsable:

- Departamento de Seguridad

4.2 Implementación de un sistema de autenticación de doble factor

El objetivo del presente proyecto es la aplicación de controles que mitiguen el impacto y/o la probabilidad de ocurrencia de las amenazas:

- [A.11] Acceso no autorizado
- [A.5] Suplantación de la identidad del usuario
- [A.22] Manipulación de programas
- [A.18] Destrucción de información

El impacto acumulado de los riesgos asociados a las anteriores amenazas es de 63.8.

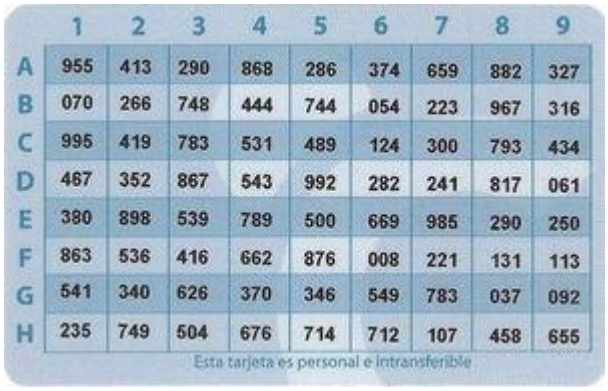
Gestión de tipo Reducción del Riesgo.

Descripción del proyecto:

El objetivo de un sistema de autenticación de doble factor es incorporar mayor fiabilidad de que el usuario que se está autenticando en un sistema es realmente el que dice ser. Con esta finalidad se incorpora al sistema una autenticación adicional. En esta autenticación adicional suele intervenir algo que posee físicamente el usuario: una tarjeta de coordenadas, un token USB, un dispositivo móvil al que llega un SMS, un dispositivo que genera códigos pseudo-aleatorios, etc. de manera que para realizar una autenticación exitosa debe intervenir algo que el usuario “sabe” y algo que el usuario “tiene”.

Existen diferentes empresas en el ámbito de la seguridad TIC que han desarrollado soluciones de autenticación de doble factor. Las soluciones de autenticación de doble factor más importantes encontramos:

- Tarjeta de códigos



	1	2	3	4	5	6	7	8	9
A	955	413	290	868	286	374	659	882	327
B	070	266	748	444	744	054	223	967	316
C	995	419	783	531	489	124	300	793	434
D	467	352	867	543	992	282	241	817	061
E	380	898	539	789	500	669	985	290	250
F	863	536	416	662	876	008	221	131	113
G	541	340	626	370	346	549	783	037	092
H	235	749	504	676	714	712	107	458	655

Esta tarjeta es personal e intransferible

Imagen 17: Tarjeta de códigos

- *Tokens* hardware o software que generan un código que solo es válido por una vez (OTP – One Time Password).

Imagen 18: Tokens hardware o software

- Otras veces la generación del OTP se ordena desde un sistema central y su envío al usuario es vía correo electrónico, SMS o *push* en app de smartphone.

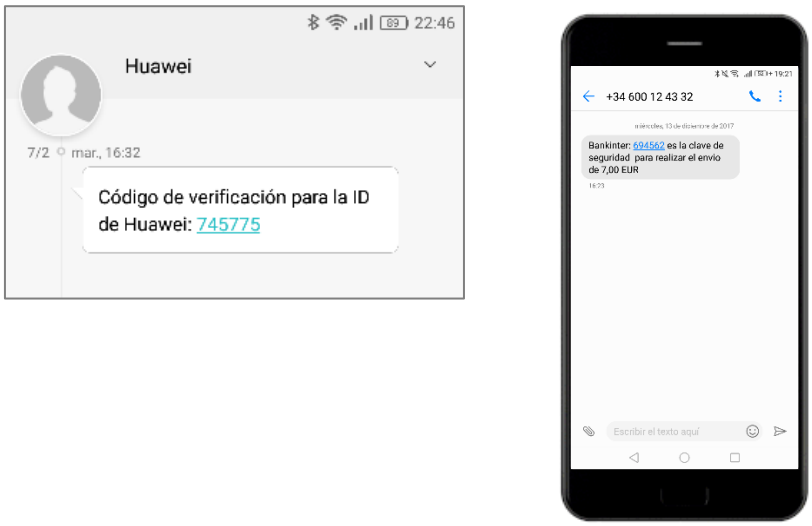


Imagen 19: OTP SMS o push en smartphone

- Solicitud de respuesta en un dispositivo (smartphone) previamente dado de alta para confirmar que se está intentando hacer uso de una cuenta.

Imagen 20: Solicitud respuesta en smartphone

Controles:

- % de despliegue de la solución de autenticación de doble factor entre los usuarios
- % de despliegue de la solución de autenticación de doble factor entre los sistemas

Duración:

- 3 meses de implantación de la solución
- 3 meses de despliegue entre los usuarios

Coste:

- Bajo

Recursos Necesarios:

- Consultor de Seguridad (10%)
- Recursos de Sistemas (por ejemplo, máquinas virtuales para albergar el sistema).
- Administrador de Sistemas (5%)

Responsable:

- Departamento de Seguridad

4.3 Implementación de un sistema DLP (Data Loss Prevention)

El objetivo del presente proyecto es la aplicación de controles que mitiguen el impacto y/o la probabilidad de ocurrencia de las amenazas:

- [A.19] Divulgación de información

El impacto acumulado de los riesgos asociados a las anteriores amenazas es de 40.8.

Gestión de tipo Reducción del Riesgo.

Descripción del proyecto:

Las soluciones de DLP permiten implementar mecanismos para controlar que información sale de la organización mediante la implementación de políticas alineadas con el negocio cuyo objetivo es la fuga de información.

Existen diversas vías de fuga de información en Integrador X. La solución a implementar deberá controlar todas ellas aplicando las mismas políticas con independencia del canal utilizado. Las posibles vías de fuga de información son:

- El correo electrónico
- Dispositivos extraíbles USBs
- La grabación de CD-ROMs, DVDs
- Subida de ficheros a páginas web o proveedores de servicios *cloud storage* (DropBox, Drive, OneDrive, etc.)
- La impresión en formato físico (papel).
- A través de formularios web
- etc.

Para poder aplicar estas reglas es necesario que la información a proteger esté debidamente clasificada. En este sentido existen diversas aproximaciones:

- Clasificación Automática:
  - Útil para la clasificación de información bien definida:
    - Información con un formato específico muy concreto
    - Información que es un extracto total o parcial de una información previamente identificada como crítica.
- Clasificación Manual:
  - Clasificación por parte del administrador del sistema en base a repositorios: sistemas de ficheros, carpetas, bases de datos, etc.
  - Clasificación bajo demanda realizada por el creador de la información.

Una vez que la solución DLP ha sido implementada, un usuario final que intente, de manera accidental o malintencionada, revelar información confidencial que ha sido etiquetada como tal, no le será permitido.

Controles:

- % de información clasificada
- Posibles canales de fuga controlados

Duración:

- 6 meses de clasificación
- 3 meses de implementación

Coste:

- Medio

Recursos Necesarios:

- Responsables de las Diferentes áreas implicadas: Áreas Comerciales y de Operaciones, para la clasificación de la información (30%)
- Consultor de Seguridad (20%)
- Recursos de Sistemas (por ejemplo, máquinas virtuales para albergar el sistema).
- Administrador de Sistemas (5%)

Responsable:

- Áreas Comerciales y de Operaciones
- Departamento de Seguridad

4.4 Impartición de formación / concienciación en el ámbito de la Seguridad de la Información

El objetivo del presente proyecto es la aplicación de controles que mitiguen el impacto y/o la probabilidad de ocurrencia de las amenazas:

- [A.19] Divulgación de información

El impacto acumulado de los riesgos asociados a las anteriores amenazas es de 40.8.

Gestión de tipo Reducción del Riesgo.

Descripción del proyecto:

La formación y concienciación en los ámbitos de seguridad de los empleados de Integrador X es de vital importancia para la seguridad de la información de la organización. Por muchas medidas técnicas de seguridad que se apliquen, el usuario siempre será el eslabón más débil de la cadena, es por ese motivo que debe este debe ser formado en el ámbito de la seguridad.

La formación a plantear en el presente proyecto debe ser planteada como una formación muy práctica de como los usuarios deben comportarse en su día a día teniendo en cuenta la seguridad. No debe limitarse a ser una formación de buenas prácticas, sino que debe incorporar ejemplos y casos de uso cercanos a su realidad para que realmente los usuarios tomen conciencia de que la seguridad es un tema del que forman parte.

Existen diversas aproximaciones a la hora de ejecutar una acción de concienciación en seguridad:

- Mediante presentaciones realizadas por personal de seguridad con un perfil que sea capaz de trasmitir las claves al resto de personal de la organización. Estas presentaciones no deberían exceder la hora u hora y media de duración para ser realmente efectivas y deberían ser realizadas a grupos de no más de 20-30 usuarios.
- Mediante videos que deba visualiza el usuario donde se traslade esta información. Uno de estos videos puede ser una de las presentaciones expuestas en el punto anterior o pequeñas píldoras monotemáticas que no impliquen mucho tiempo al usuario para su visualización.
- Mediante píldoras formativas monotemáticas que el usuario realice bajo demanda, donde se le haga una explicación de un tema concreto (seguridad en el correo electrónico, con los dispositivos extraíbles, como actuar para evitar fugas de información, etc.) que luego será puesto en práctica a través de una sesión interactiva con el usuario.

En los diferentes casos expuestos anteriormente es conveniente, en la medida de lo posible, la particularización de las formaciones en función de los perfiles a los que dirija.

En cualquier caso, debe llevarse un control del personal que ha realizado la formación y asegurar que la totalidad del personal designado para la realización de las sesiones formativas acabe realizándola.

Es conveniente que estas sesiones formativas se repitan de manera periódica de manera que se refresque la formación de los usuarios según la actualización de los temarios.

Controles:

- % de usuarios objetivo que han realizado la correspondiente formación en el último año.

Duración:

- 1 mes en la preparación del temario
- 3 meses en la formación de los diferentes usuarios.

Coste:

- Bajo

Recursos Necesarios:

- Consultor de Seguridad (30%)
- Responsables de las Diferentes áreas implicadas: Áreas Comerciales y de Operaciones (5%)

Responsable:

- Departamento de Seguridad
- Áreas Comerciales y de Operaciones

4.5 Implementación de un sistema de backup de la información en *cloud*

El objetivo del presente proyecto es la aplicación de controles que mitiguen el impacto y/o la probabilidad de ocurrencia de las amenazas:

- [A.18] Destrucción de información
- [A.24] Denegación de servicio
- [E.24] Caída del sistema por agotamiento de recursos

El impacto acumulado de los riesgos asociados a las anteriores amenazas es de 16.8.

Gestión de tipo Reducción del Riesgo.

Descripción del proyecto:

En el caso de Integrador X, en el que la organización ha tomado la decisión de trabajar con soluciones en *cloud*, el almacenamiento de la información de la compañía esta delegado en las empresas prestadoras de este tipo de servicios, Google en el caso que nos ocupa.

A pesar de estar la disponibilidad prácticamente garantizada gracias a los SLAs incorporados en los contratos firmados con este tipo de empresas, esta alta disponibilidad del servicio no protege a la organización de las anteriores amenazas:

- [A.18] Destrucción de información: Por descuido, o de manera intencionada, se puede dar el caso de que se elimine información almacenada en estos servicios en *cloud*.
- [A.24] Denegación de servicio: Puede existir un ataque de denegación de servicio tanto en la parte del prestador del servicio como en la parte de la conexión correspondiente a Integrador X.
- [E.24] Caída del sistema por agotamiento de recursos: Existe la posibilidad -a priori remota- de que el prestador de servicios en *cloud* agote sus recursos y la disponibilidad del servicio se vea comprometida.

El proyecto propuesto en el presente punto debe proporcionar un sistema capaz de realizar, de manera periódica, una copia de seguridad local de la información albergada en el *cloud*. De esta manera, en el caso de materializarse alguna de las anteriores amenazas, Integrador X dispondría de un sistema de contingencia que le permitiría continuar con su actividad -al menos para aquellos procesos de mayor criticidad a los que se deberá aplicar esta medida.

Controles:

- % de datos con copia local
- Diferencia temporal entre la imagen en el cloud y su copia local

Duración:

- 3 meses para la preparación de la infraestructura
- 1 mes para la realización de la primera copia de seguridad

Coste:

- Medio

Recursos Necesarios:

- Arquitecto de Sistemas (10%)
- Administrador de Sistemas (30%)
- Recursos de Sistemas (por ejemplo, sistema de almacenamiento para albergar las copias de seguridad).
- Administrador de Comunicaciones (10%)
- Consultor de Seguridad (5%)

Responsable:

- Departamento de Sistemas

4.6 Implantación de sistemas Antimalware, ZeroDay, anti-APT, etc.

El objetivo del presente proyecto es la aplicación de controles que mitiguen el impacto y/o la probabilidad de ocurrencia de las amenazas:

- [E.8] Difusión de software dañino

El impacto acumulado de los riesgos asociados a las anteriores amenazas es de 12.

Gestión de tipo Reducción del Riesgo.

Descripción del proyecto:

Si bien es verdad que la mayoría de organizaciones disponen de soluciones de antivirus/antimalware en su infraestructura (en los puestos de trabajo, en servidores, elementos perimetrales, etc.), cada vez más, estas medidas son insuficientes para luchar contra las nuevas amenazas que acechan en la actualidad a las organizaciones.

La medida propuesta consiste en la implantación de sistemas de protección antimalware avanzado, ataques de día cero (ZeroDay) y amenazas persistentes avanzadas (APT, Advanced Persistent Threat) para luchar contra estas nuevas amenazas. Está demostrado que las protecciones basadas en firmas conocidas, como venían funcionando los antivirus tradicionales, ya no son suficientes. Las organizaciones deben incorporar a su infraestructura sistemas de detección de amenazas más avanzadas como podrían ser las soluciones basadas en el análisis de comportamiento.

Existen diferentes aproximaciones a la hora de afrontar la incorporación de este tipo de protecciones adicionales:

- Protección del equipo: EndPoint o Servidor
- Protección perimetral mediante la explotación en un entorno controlado (*sandbox*) de los contenidos sospechosos

Ambas aproximaciones son complementarias ya que cubren vías de infección diferentes y la capacidad de análisis y actuación en cada caso varía:

- Protección en el propio equipo:
  - Es el sitio donde, si existe realmente un malware, este va a intentar ejecutarse.
  - Es posible que tengamos, al menos, un paciente cero (primer equipo infectado) antes de poder determinar que realmente se trataba de un malware.
  - Cubre amenazas que puedan haber llegado por múltiples vías: correo, navegación, USB, infección horizontal (a través de la red local), etc.
- Protección perimetral:
  - Permite detectar la amenaza previamente a su llegada al equipo del usuario final siempre y cuando la vía de entrada sea a través de la comunicación con el exterior: correo electrónico, navegación, descarga de ficheros, etc.
  - La explotación de la amenaza en un entorno de *sandboxing* puede no ser concluyente: con la intención de no ser detectados por este tipo de entornos, los programas maliciosos son capaces de: emular un comportamiento "adecuado" si detectan que están siendo ejecutados en un entorno de *sandboxing*, tener un inicio retrasado de la ejecución del código malicioso, etc.
  - Para el análisis de la totalidad del tráfico que entra en la organización, se debe disponer de un sistema que permita inspeccionar el tráfico cifrado (cada vez más abundante).

Controles:

- Nº de incidentes causados por código malicioso tratados por el equipo de respuesta a incidentes.

Duración:

- 2 meses de instalación de la plataforma, definición de políticas y pilotaje de la solución
- 1 mes de despliegue

Coste:

- Medio

Recursos Necesarios:

- Consultor de Seguridad (30%)
- Recursos de Sistemas (por ejemplo, máquinas virtuales para albergar el sistema).
- Administrador de Sistemas (5%)

Responsable:

- Departamento de Seguridad

4.7 Contratación de los Servicios de un CPD de respaldo

El objetivo del presente proyecto es la aplicación de controles que mitiguen el impacto y/o la probabilidad de ocurrencia de las amenazas:

- [N.*] Desastres naturales

El impacto acumulado de los riesgos asociados a las anteriores amenazas es de 6.4.

Gestión de tipo Reducción del Riesgo.

Descripción del proyecto:

Para aquellos activos vitales para el negocio que sean susceptibles a la amenaza que supone la materialización de un desastre natural que afecte al CPD de Integrador X será conveniente la contratación de aquellos servicios que garanticen la continuidad de negocio de Integrador X en el caso de materializarse dicha amenaza.

Deberán seleccionarse qué activos han de replicarse en el centro que preste los servicios de continuidad de negocio definiendo, junto con negocio, los principales parámetros del servicio a contratar. En este tipo de servicios parte de los parámetros más habituales son:

- RPO (Recovery Point Objective): El RPO determina el objetivo de posible pérdida máxima de datos desde el punto posible de recuperación posible hasta la caída del sistema. No depende del tiempo de recuperación.
- RTO (Recovery Time Objective): Es el tiempo durante el cual una organización puede tolerar la falta de funcionamiento de sus aplicaciones sin afectar a la continuidad del negocio.

Entre las diferentes estrategias a seguir para este proyecto tenemos:

- *Cold Site*, *Warm Site*, *Hot Site*: En la que se dispone de una segunda ubicación con diferentes niveles de preconfiguración/preparación para el inicio del servicio ante una contingencia:
  - desde la menos preparada, *Cold Site*, en la que únicamente se disponen de los servicios básicos: cableado, sistemas de aire acondicionado, etc.,
  - hasta la más preparada, *Hot Site*, donde disponemos de todos los elementos necesarios para la prestación del servicio en contingencia, disponiendo incluso de una copia reciente de la última información necesaria para la prestación del servicio.
- Ubicaciones móviles de tipo remolques o contenedores.
- Acuerdos recíprocos entre diferentes compañías en las que se acuerdan proveerse mutuamente de instalaciones en caso de emergencia.

Debido a que el objetivo del presente plan es hacer frente a la amenaza que supone la materialización de un desastre natural, la selección de la ubicación del CPD que garantice la

continuidad del negocio deberá tener muy en cuenta la distancia geográfica entre el CPD principal y el de respaldo de manera que se minimice al máximo la probabilidad de que el mismo desastre natural pueda afectar a ambos centros de datos. Por contra, una mayor distancia entre los CPDs implica sobrecostes en comunicaciones, retardos, inconvenientes logísticos, etc. que también deberán ser tenidos en cuenta.

Para validar la correcta definición del Plan de Contingencia, éste deberá ser testeado periódicamente, añadiendo complejidad con el tiempo y simulando cada vez con mayor realismo una situación de contingencia.

Controles:

- Resultados de los test del plan

Duración:

- 3 meses para la definición del Plan
- 6 meses para la implementación
- 3 meses para el ajuste fino tras los primeros test

Coste:

- Alto

Recursos Necesarios:

- Consultor de Seguridad (50%)
- Arquitecto de Sistemas (30%)
- Consultor de Sistemas (40%)
- Arquitecto de Comunicaciones (20%)
- Consultor de Comunicaciones (30%)

Responsable:

- Departamento de Seguridad
- Departamento de Sistemas
- Departamento de Comunicaciones

4.8 Implantación de un sistema de Anti-DDoS

El objetivo del presente proyecto es la aplicación de controles que mitiguen el impacto y/o la probabilidad de ocurrencia de las amenazas:

- [A.24] Denegación de servicio

El impacto acumulado de los riesgos asociados a las anteriores amenazas es de 5.6.

Gestión de tipo Reducción del Riesgo.

Descripción del proyecto:

Debido a la alta dependencia de Integrador X del software consumido en formato servicio, la protección ante un ataque de denegación de servicio es de suma importancia para la continuidad del negocio: en el caso de materializarse la amenaza, la organización estaría incapacitada para el uso de dichos servicios.

Un ataque de denegación de servicio que afecte al negocio de Integrador X, puede darse tanto en el lado del prestador del servicio -Google, en el caso que nos ocupa- como en el lado de Integrador X.

En el primer caso la capacidad de maniobra de Integrador X queda limitada a la revisión de los SLAs -y penalizaciones asociadas- reflejados en los contratos entre Integrador X y Google, comprobando que estos se alinean con los requerimientos de negocio y en caso contrario renegociando estos SLAs (en la medida de lo posible). Esta propuesta de acción queda detallada en el posterior punto 4.10.

En el segundo caso: en el que exista un ataque de denegación de servicio en el lado de Integrador X, la organización deberá estar preparada para responder a dicho ataque y restablecer el servicio en el menor tiempo posible.

Un ataque de denegación de servicio consiste en el desmesurado consumo ilícito de los recursos de un sistema (equipo/s, enlace de comunicaciones, etc.) de manera que éste no dispone de recursos suficientes para atender las peticiones lícitas. Existen diferentes aproximaciones a la hora de abordar este tipo de amenazas:

- Con infraestructura *on-premise*[10] que detecta las peticiones ilícitas y las descarta antes de que éstas lleguen al sistema al que son dirigidas. Este sistema permite un gran control pero por contra tiene la limitación del enlace de entrada que puede ser saturado con independencias de la capacidad del hardware instalado en las dependencias de la organización.
- En modalidad servicio en el *cloud* la totalidad del tráfico de la organización es redirigido al servicio en el *cloud* que discrimina si es tráfico lícito, y lo redirige a la organización, o si por el contrario es tráfico ilícito, y lo descarta. Esta modalidad añade un pequeño retardo ya que la totalidad del tráfico debe traspasar el servicio en el *cloud* previamente a llegar a la organización a la que va dirigido.
- En modalidad híbrida de manera que en una primera instancia se intenta hacer frente al ataque desde la infraestructura *on-premise*, y en caso de que el ataque amenace con sobrepasar la capacidad del hardware *on-premise* o del enlace de estrada, el servicio pasa a prestarse en el *cloud*.

Es muy común que este tipo de servicios sean prestados por los propios operadores de comunicaciones según la segunda modalidad planteada. Con esta opción se reduce el posible retardo introducido por el hecho de derivar el tráfico a un servicio *cloud* externo puesto que el servicio es prestado por el propio operador de comunicaciones.

[10] Mediante infraestructura en local

Controles:

- Nº de incidentes causados por un ataque de denegación de servicio tratados por el equipo de respuesta a incidentes.

Duración:

- 3 meses

Coste:

- Bajo

Recursos Necesarios:

- Consultor de Seguridad (20%)
- Consultor de Sistemas (10%)
- Consultor de Comunicaciones (5%)

Responsable:

- Departamento de Seguridad

4.9 Implementación de redundancia / alta disponibilidad en las comunicaciones corporativas

El objetivo del presente proyecto es la aplicación de controles que mitiguen el impacto y/o la probabilidad de ocurrencia de las amenazas:

- [I.8] Fallo de servicios de comunicaciones

El impacto acumulado de los riesgos asociados a las anteriores amenazas es de 5.6.

Gestión de tipo Reducción del Riesgo.

Descripción del proyecto:

Debido a la alta dependencia de Integrador X del software consumido en formato servicio a través de la red, la conectividad de la organización a Internet es de vital importancia para la continuidad del negocio: en el caso de materializarse la amenaza, la organización estaría incapacitada para el uso de dichos servicios.

El presente proyecto consiste en dotar a la organización de un enlace redundante de acceso a Internet con el objetivo de minimizar el impacto en el caso de materializarse el riesgo.

A la hora de definir en detalle este proyecto se han de tener en cuenta diversas consideraciones:

- ¿Se va a utilizar una solución diversificada geográficamente? Esta alternativa incrementa la complejidad del proyecto, pero la hace más robusta en los casos en que la incomunicación sea motivada por una problemática local (como podrían ser obras en la zona).
- ¿Se utilizará un operador de telecomunicaciones diferente al principal o por el contrario se va a utilizar el mismo? En el primer caso el proyecto proporciona mayor robustez a la solución global. En el segundo, la gestión económica con un único interlocutor puede revertir en beneficios económicos a Integrador X.
- ¿La solución de backup va a disponer de la misma capacidad que la principal? Si se decide optar por una solución de contingencia en la que se sacrifique parte del rendimiento, se podrán obtener beneficios económicos, pero por el contrario se deberá evaluar bien las necesidades de la organización en situación de contingencia.

Para validar la correcta definición del Plan de Contingencia, éste deberá ser testeado periódicamente, añadiendo complejidad con el tiempo y simulando cada vez con mayor realismo la situación de contingencia.

Controles:

- Resultados de los test del plan

Duración:

- 3 meses

Coste:

- Bajo

Recursos Necesarios:

- Arquitecto de Comunicaciones (10%)
- Consultor de Comunicaciones (20%)
- Consultor de Seguridad (5%)

Responsable:

- Departamento de Comunicaciones

4.10 Definición de ANS (o SLA) acordes con los requerimientos del negocio

El objetivo del presente proyecto es la aplicación de controles que mitiguen el impacto y/o la probabilidad de ocurrencia de las amenazas:

- [A.24] Denegación de servicio
- [E.24] Caída del sistema por agotamiento de recursos

El impacto acumulado de los riesgos asociados a las anteriores amenazas es de 11.2.

Gestión de tipo Transferencia del Riesgo.

Descripción del proyecto:

Tal y como se ha constatado en anteriores apartados, existe una alta dependencia de Integrador X con los servicios prestados en *cloud*. En algunos casos, Integrador X puede tomar medidas con el objetivo de minimizar el impacto en el caso de materializarse un riesgo; en otros, sencillamente, es técnicamente imposible.

En estos últimos casos la única alternativa a disposición de Integrador X es asegurarse que, por parte de los prestadores de servicios, éstos cumplirán con unos acuerdos de nivel de servicio (ANS). Para ello, Integrador X deberá asegurarse que contractualmente los ANS definidos, y las penalizaciones en caso de incumplimiento, estén alineadas con los requerimientos del negocio. En caso contrario se deberá abrir un proceso de negociación con los proveedores de servicio para proceder a la modificación de estos ANS.

Controles:

- Tiempo transcurrido desde la última revisión de ANS y haber validado su alineamiento con los requerimientos de la organización.
- % ANS alineados con los requerimientos de seguridad de SGSI

Duración:

- 1 mes

Coste:

- Bajo

Recursos Necesarios:

- Responsables de las Diferentes áreas implicadas: Áreas Comerciales y de Operaciones (10%)
- Consultor de Seguridad (10%)

Responsable:

- Áreas Comerciales y de Operaciones
- Departamento de Seguridad

4.11 Contratación de seguro con cobertura de los Desastres Naturales en el ámbito del CPD

El objetivo del presente proyecto es la aplicación de controles que mitiguen el impacto y/o la probabilidad de ocurrencia de las amenazas:

- [N.*] Desastres naturales

El impacto acumulado de los riesgos asociados a las anteriores amenazas es de 6.4.

Gestión de tipo Transferencia del Riesgo.

Descripción del proyecto:

Existe la opción de transferir ciertos riesgos a pólizas aseguradoras. Los seguros en este ámbito están indicados para los riesgos de menor probabilidad y mayor impacto, aquellos para los cuales poner otras medidas es menos rentable que contratar un seguro que cubra las pérdidas en caso de que se materialicen estos riesgos.

En el caso del riesgo que nos ocupa, para la materialización de un desastre natural que afecte al CPD de Integrador X ya se ha propuesto en el punto 4.7 un proyecto con el objetivo de reducir este riesgo. Esto no implica que ambos proyectos sean excluyentes, es más, se podría considerar que son complementarios ya que, aunque se cuente con los servicios de un CPD de respaldo siempre existirá una afectación (en función del RPO y RTO que se definan para dicho proyecto) que puede ser cubierta por la póliza.

La aseguradora deberá valorar el impacto de los riesgos a cubrir, el índice de siniestralidad, etc. Exigirán a Integrador X cumplir una serie de medidas de seguridad incluso ofrecerán cierto nivel de descuento en el caso de tomar medidas que minimicen el riesgo -como se indicaba en el anterior párrafo con la implementación del proyecto descrito en el punto 4.7.

En cualquier caso, a la hora de contratar un seguro se deberán revisar las coberturas, los términos y las exclusiones de éste y ver si están alineados con las necesidades de la organización.

Controles:

- Tiempo transcurrido desde la última revisión de las coberturas, términos y exclusiones y haber validado su alineamiento con los requerimientos de la organización.

Duración:

- 1 mes

Coste:

- Bajo

Recursos Necesarios:

- Consultor de Seguridad (10%)
- Consultor de Sistemas (10%)

Responsable:

- Departamento de Seguridad
- Departamento de Sistemas

4.12 Planificación de Proyectos de Mejora de la Seguridad de la Información

En el presente apartado se propondrá una planificación para la ejecución de los proyectos definidos en los apartados anteriores y cuyo objetivo es la reducción de los riesgos determinados a partir del análisis de riesgos, detallado en el punto 3, por debajo del nivel aceptado por la organización.

En primera instancia se analizará la información relevante relativa a los proyectos de mejora, información detallada en los puntos anteriores, con el objetivo de facilitar la toma de decisiones al respecto de qué proyectos deberán ser abordados, con qué prioridad o priorización y, en definitiva, con qué planificación.

De manera esquemática los principales datos de los proyectos propuestos para la mitigación de los riesgos que superan el umbral aceptado por la organización es el detallado en la siguiente tabla.

Proyecto	**Impacto reducido/ mitigado**	**Duración (meses)**	**Coste**
Implementación de un sistema criptográfico corporativo de clave pública (PKI) acompañado de una solución de cifrado de la información y las comunicaciones	92,6	12	Medio
Implementación de un sistema de autenticación de doble factor	63,8	6	Bajo
Implementación de un sistema DLP (Data Loss Prevention)	40,8	9	Medio
Impartición de formación / concienciación en el ámbito de la Seguridad de la Información	40,8	4	Bajo
Implementación de un sistema de backup de la información en cloud	16,8	4	Medio
Implantación de sistemas Antimalware, ZeroDay, anti-APT	12	3	Medio
Contratación de los Servicios de un CPD de respaldo	6,4	12	Alto
Implantación de un sistema de Anti-DDoS	5,6	3	Bajo
Implementación de redundancia / alta disponibilidad en las comunicaciones corporativas	5,6	3	Bajo
Definición de ANS (o SLA) acordes con los requerimientos del negocio	11,2	1	Bajo
Contratación de seguro con cobertura de los Desastres Naturales en el ámbito del CPD	6,4	1	Bajo

Tabla 14: Resumen de proyectos propuestos

En la siguiente imagen se puede observar de manera gráfica la misma información detallada en la tabla anterior: para cada proyecto, en el eje de abscisas (x) podemos observar la duración estimada en meses, en el eje de ordenadas (y) se ordenan los proyectos en función de su coste estimado y el tamaño de la representación de cada proyecto proporciona una idea del impacto a reducir/mitigar con cada uno de ellos.

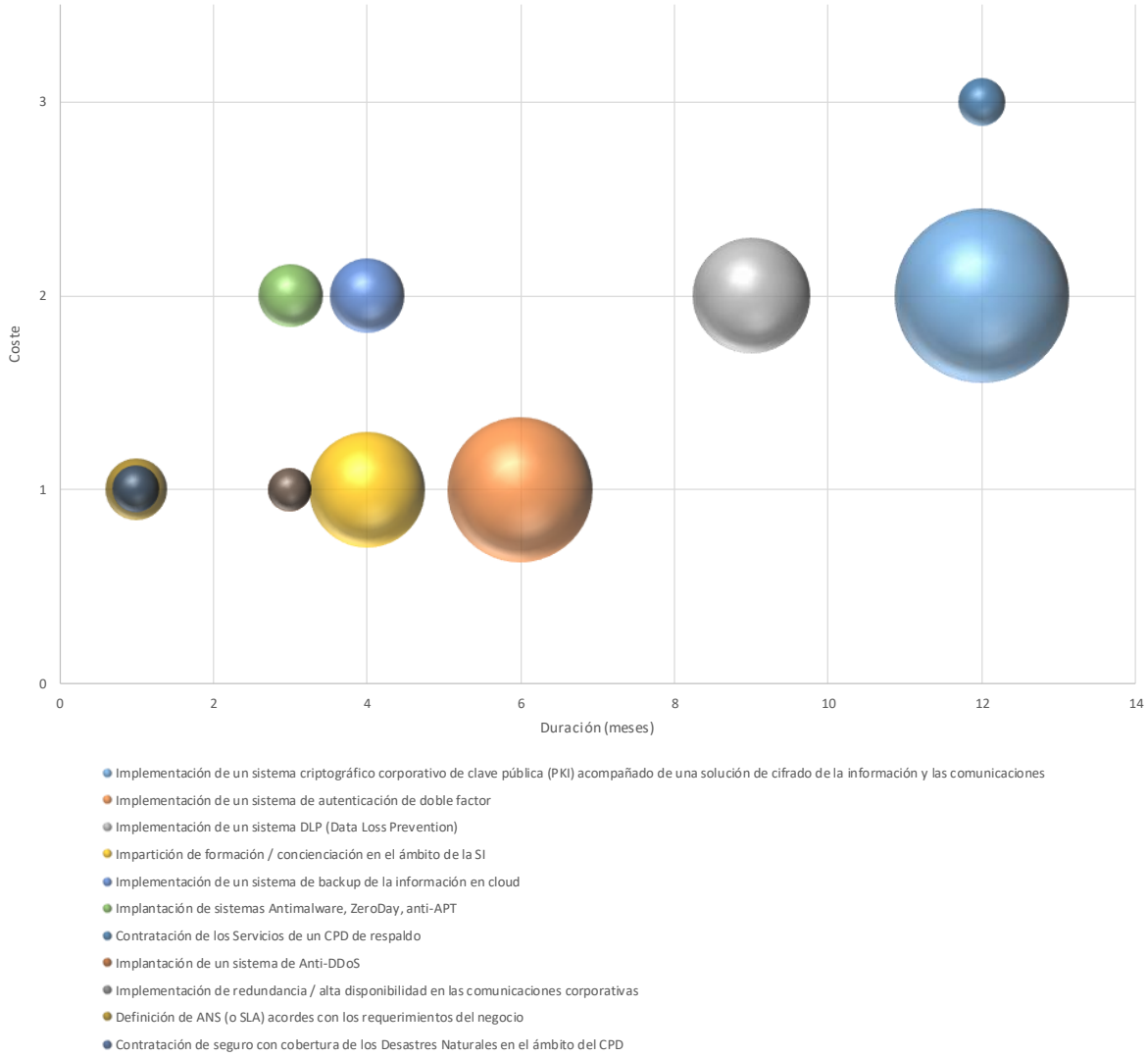


Imagen 21: Resumen de proyectos propuestos

De la anterior representación gráfica se extraen las siguientes conclusiones:

- Los *Quick Wins*, es decir, proyectos de rápida ejecución y bajo coste que reportarán un beneficio rápido son:
  - Definición de ANS (o SLA) acordes con los requerimientos del negocio
  - Contratación de seguro con cobertura de los Desastres Naturales en el ámbito del CPD
  - Implantación de un sistema de Anti-DDoS
  - Implementación de redundancia / alta disponibilidad en las comunicaciones corporativas
  - Impartición de formación / concienciación en el ámbito de la Seguridad de la Información
  - Implementación de un sistema de autenticación de doble factor

  Estos proyectos son candidatos a ser ejecutados en primera instancia.

- En el otro extremo, proyectos de dilatada implantación y alto coste, encontramos el proyecto de Contratación de los Servicios de un CPD de respaldo. En este sentido además se da la coincidencia de que es un proyecto en el que el impacto a reducir/mitigar es bajo.
  Este es un proyecto candidato a ser descartado o con una baja priorización.
  Por otro lado se da la coincidencia de que ya existe otro proyecto (Contratación de seguro con cobertura de los Desastres Naturales en el ámbito del CPD) cuyo objetivo es mitigar las mismas amenazas.

- Entremedias quedan el resto de proyectos que deberán ser priorizados en base a la información proporcionada en el presente documento y a las prioridades de cada momento de Integrador X.

A partir de poner en común las anteriores conclusiones junto con la dedicación de recursos requeridos para los diferentes proyectos y la dedicación requerida por parte del departamento responsable de cada uno de ellos, se plantea la siguiente planificación como una propuesta para la ejecución de los diferentes proyectos.

Imagen 22: Gantt: Propuesta ejecución proyectos de mejora

5. AUDITORÍA DE CUMPLIMIENTO

El objetivo del presente apartado es analizar como la implantación de los proyectos de mejora definidos en el apartado anterior ha afectado en el cumplimiento de Integrador X en el ámbito de la ISO/IEC 27000.

La situación inicial de la organización previamente a la implantación del SGSI detallado a lo largo del presente documento es el detallado en el apartado 1.3, y sus correspondientes subapartados. En los próximos apartados se expone el resultado de la ejecución de una auditoria interna, según se define en el documento "MuñozMercaderEDGAR_TFM_Procedimiento de Auditorias v1.1", y que detallará la situación de Integrador X tras la implantación del SGSI y de los proyectos de mejora definidos.

5.1 Objetivo de la Auditoría

Los objetivos perseguidos por el programa de auditorías son revisar el cumplimiento de los controles establecidos en el SGSI, identificar posibles incumplimientos proporcionando información que pueda ser indicio al respecto de las causas de estos incumplimientos y disponer de una visión actualizada del nivel de seguridad proporcionado por la infraestructura de TI que soporta los activos de información contemplados en el SGSI.

El resultado de la presente auditoría será puesto en conocimiento de la Dirección según el procedimiento revisión por la Dirección definido para el presente SGSI.

5.2 Alcance de la Auditoría

La presente auditoría se centra en los procesos relacionados con la actividad de las Áreas Comerciales y de Operaciones y los sistemas de Tecnologías de la Información utilizados por estas áreas para el desarrollo de sus funciones.

5.3 Criterios de la Auditoría

Los criterios a seguir a la hora de realizar la presente auditoría son los marcados por las políticas de seguridad y guías de buenas prácticas definidas dentro del SGSI, que a su vez utilizan como marco de trabajo la familia de normas ISO/IEC 27000-2013.

5.4 Equipo Auditor

La presente auditoría, esta ha sido realizada por personal del departamento de Seguridad. Es importante destacar que el departamento de Seguridad está totalmente desligado de las operativas de las áreas de análisis lo que garantiza la máxima trasparencia y objetividad en el resultado de las auditorías.

El rol de auditor jefe ha sido desarrollado por el CISO de Integrador X disponiendo bajo su responsabilidad en el transcurso de la presente auditoría de una persona del departamento con perfil auditor de cumplimiento normativo ISO/IEC 27001-2013.

A grandes rasgos, el auditor interno, dispone de la siguiente formación/certificaciones y experiencia:

- Formación Universitaria en Ingeniería Informática o Telecomunicaciones
- Formación específica en ISO/IEC27001: ISO/IEC27001 Lead Auditor

- Experiencia en la realización de auditorías de al menos 5 años
- Conocimientos en GDPR.

5.5 Fecha y Lugar de Realización de la Auditoría

La auditoría ha sido realizada principalmente en las dependencias centrales de Integrador X en Madrid, aunque alguna de las entrevistas realizadas ha contemplado personal de las áreas de las Áreas Comerciales y de Operaciones de otras delegaciones: Barcelona, Bilbao y Valencia.

La auditoría fue realizada el durante el pasado mes de mayo de 2018.

5.6 Hallazgos y Evidencias Identificados

A continuación se detallan los hallazgos y evidencias identificadas durante la ejecución de la auditoría. La auditoría se ha centrado en la revisión de los controles definidos de manera global para el SGSI, tal y como se define en el “MuñozMercaderEDGAR_TFM_Gestion de Indicadores v1.1.pdf”, y para cada uno de los proyectos definidos en el ámbito del presente SGSI.

- Indicadores globales
  - % de cumplimiento de los procesos según definición en el SGSI: No se disponen de mecanismos que permitan la medida del indicador.
  - % de incumplimiento por carencias tecnológicas: No se disponen de mecanismos que permitan la medida del indicador.
  - % de incumplimiento por carencias procedimentales: No se disponen de mecanismos que permitan la medida del indicador.
  - % de incumplimiento por carencia de recursos: No se disponen de mecanismos que permitan la medida del indicador.
  - % de los incumplimientos que ponen en riesgo la Confidencialidad de la información: No se disponen de mecanismos que permitan la medida del indicador.
  - % de los incumplimientos que ponen en riesgo la Integridad de la información: No se disponen de mecanismos que permitan la medida del indicador.
  - % de los incumplimientos que ponen en riesgo la Disponibilidad de la información: No se disponen de mecanismos que permitan la medida del indicador.
  - % de los incumplimientos que ponen en riesgo la Autenticidad de la información: No se disponen de mecanismos que permitan la medida del indicador.
  - % de los incumplimientos que ponen en riesgo la Trazabilidad de la información: No se disponen de mecanismos que permitan la medida del indicador.
  - % de personal que ha realizado las sesiones de concienciación: **95%**
  - Valoración de los sujetos entrevistados de la utilidad del Plan de Concienciación: **Útil** (rango de valores posibles: Nada útil, Poco útil, Algo útil, Útil, Muy útil).
  - % de personal que conoce de la existencia de las Políticas de SI y conoce su contenido: **96%**
- Implementación de un sistema criptográfico corporativo de clave pública (PKI) acompañado de una solución de cifrado de la información y las comunicaciones
  - % de usuarios / sistemas con certificado emitido: **98%** de los usuarios disponen de un certificado emitido (por indisponibilidades varias, se encuentra desplegado en el 90%).

- % de información cifrada almacenada: **20%** (en un entorno de piloto).
- % de comunicaciones cifradas: **40%**. Sólo en las comunicaciones site-to-site.

- Implementación de un sistema de autenticación de doble factor
  - % de despliegue de la solución de autenticación de doble factor entre los usuarios: **98%** de los usuarios ya están dados de alta para poder hacer uso de la autenticación de doble factor.
  - % de despliegue de la solución de autenticación de doble factor entre los sistemas: **40%**. El despliegue de la autenticación de doble factor se ha llevado a cabo en una primera fase en los entornos *on-premise*. En una segunda fase se procederá a su implementación en los sistemas albergados en la nube o soluciones *as a service*.
- Implementación de un sistema DLP (Data Loss Prevention)
  - % de información clasificada: **80%**. La clasificación ha sido realizada en base a contenedores, se ha de contemplar que no toda la información esté correctamente clasificada.
  - Posibles canales de fuga controlados: **2**: Dispositivos extraíbles y navegación (no cifrada).
- Impartición de formación / concienciación en el ámbito de la Seguridad de la Información
  - % de usuarios objetivo que han realizado la correspondiente formación en el último año: **95%**
- Implementación de un sistema de backup de la información en cloud
  - % de datos con copia local: **100%**
  - Diferencia temporal entre la imagen en el cloud y su copia local: **1 día**
- Implantación de sistemas Antimalware, ZeroDay, anti-APT, etc.
  - Nº de incidentes causados por código malicioso tratados por el equipo de respuesta a incidentes: **5 casos semanales**. En general se tratan de casos puntuales sin una propagación destacable dentro de la organización.
- Contratación de los Servicios de un CPD de respaldo
  - Resultados de los test del plan: **El CPD de respaldo no ha sido puesto en producción**.
- Implantación de un sistema de Anti-DDoS
  - Nº de incidentes causados por un ataque de denegación de servicio tratados por el equipo de respuesta a incidentes: **0**. La totalidad de los ataques de DDoS han podido ser mitigados.
- Implementación de redundancia / alta disponibilidad en las comunicaciones corporativas
  - Resultados de los test del plan: **El informe del último test ejecutado da un resultado satisfactorio**.
- Definición de ANS (o SLA) acordes con los requerimientos del negocio
  - Tiempo transcurrido desde la última revisión de ANS y haber validado su alineamiento con los requerimientos de la organización: **9 meses**.
  - % ANS alineados con los requerimientos de seguridad de SGSI: **100%**

- Contratación de seguro con cobertura de los Desastres Naturales en el ámbito del CPD
  - Tiempo transcurrido desde la última revisión de las coberturas, términos y exclusiones y haber validado su alineamiento con los requerimientos de la organización: **9 meses**.

5.7 Conclusiones

Por lo general los proyectos de mejora definidos al amparo del SGSI han sido desplegados satisfactoriamente y según planificación inicialmente definida.

El proyecto de mejora consistente en la contratación un CPD de respaldo no ha sido implementado; según la planificación inicial, su implementación estaba prevista en dos años (1 año después de la presente auditoría).

Los indicadores de cada uno de los controles, por norma general, se encuentran dentro de los parámetros esperados. Será de especial interés analizar la evolución de estos indicadores en futuras auditorías y analizar si existe una evolución, una estabilización / estancamiento o una involución de éstos.

Es necesario destacar los indicadores asociados al proyecto de mejora “Implementación de un sistema criptográfico corporativo de clave pública (PKI) acompañado de una solución de cifrado de la información y las comunicaciones”. La puesta en marcha de este tipo de soluciones no es posible sin un despliegue del 100%, o muy próximo, de la solución entre todos usuarios; en caso contrario, los usuarios que no dispongan de la solución desplegada no podrían acceder a la información cifrada.

5.8 Grado de Cumplimiento

Al igual que se hizo en los puntos 1.3.1 y 1.3.2, para determinar el grado de cumplimiento se determinará el nivel de madurez en base a los niveles definidos por CMM mostrados en la Tabla 1.

5.8.1 Requerimientos ISO/IEC 27001

La ISO/IEC 27001 define 7 grupos de requerimientos para establecer, implementar, mantener y mejorar de manera continua un SGSI en una organización. Tras la implantación de SGSI detallado en el presente documento la evolución en el cumplimiento de estos requerimientos es el detallado a continuación.

5.8.1.1 Contexto de la Organización

- Entendimiento de la organización y su contexto: La implantación del SGSI no implica una mejora en el presente requerimiento.
- Entendimiento de las necesidades y expectativas de las partes interesadas: La implantación del SGSI conlleva un mayor conocimiento de las necesidades y expectativas de las partes interesadas. La realización del análisis de riesgos aporta una visión clara de las necesidades de la organización.
- Definición del alcance del SGSI: El alcance del SGSI queda definido y se establece como referencia para la evolución continua de éste.
- Sistema de Gestión de la Seguridad de la Información: Integrador X, tras la implementación de los proyectos de mejora, ya no se encuentra en una fase temprana de la implementación del SGSI.

5.8.1.2 Liderazgo

- Liderazgo y compromiso: Existe un compromiso por parte de la Dirección. Compromiso definido en el documento anexo “MuñozMercaderEDGAR_TFM_Roles y Responsabilidades v1.1” y revisado periódicamente según se define en el documento “MuñozMercaderEDGAR_TFM_Procedimiento Revision por Direccion v1.1”.
- Políticas de Seguridad de la Información: Existen, y queda disponible para la totalidad de la organización, las Políticas de Seguridad de la Información. Éstas están definidas en el documento “MuñozMercaderEDGAR_TFM_Politica_Seguridad de la Informacion v1.1”.
- Roles organizativos, responsabilidades y autoridades: Existe una asignación de roles, responsabilidades y autoridades relativas a la Seguridad de la Información. Dicha asignación queda reflejada en el documento “MuñozMercaderEDGAR_TFM_Roles y Responsabilidades v1.1”.

5.8.1.3 Planificación

- Acciones para la gestión de riesgos y oportunidades: En el ámbito del SGSI se ha desarrollado un análisis de riesgos, inexistente hasta el momento.
- Definición de objetivos en la Seguridad de la Información y planificación para su consecución: A raíz del análisis de riesgos al que se hace referencia en el anterior punto, se han definido una serie de proyectos de mejora para aquellos riesgos que han quedado por encima del umbral aceptado por la organización. Estos proyectos han sido planificados en base a criterios de costes, duración e impacto en la seguridad de la organización.

5.8.1.4 Soporte

- Recursos: La implantación del SGSI no implica una mejora en el presente requerimiento.
- Competencia: La implantación del SGSI no implica una mejora en el presente requerimiento.
- Concienciación: A pesar de incorporarse, dentro de los proyectos de mejora, un proyecto relativo a la formación/concienciación de los empleados, la situación previa de Integrador X en este requerimiento ya era buena. Por tanto, la implantación del SGSI no implica una mejora en el presente requerimiento.
- Comunicación: La implantación del SGSI no implica una mejora en el presente requerimiento.
- Documentación: Tras la implantación del SGSI es posible afirmar que ya se dispone de documentación relativa a la aplicación de éste. Esta queda anexa al presente documento.

5.8.1.5 Operación

- Planificación y Control Operacional: Tras la implantación del SGSI ya se dispone de una primera consciencia de los procesos.
- Evaluación de Riesgos asociados a la Seguridad de la Información: Al amparo del presente SGIS se ha realizado una primera evaluación de riesgos asociados a la Seguridad de la Información.
- Gestión de Riesgos asociados a la Seguridad de la Información: En este punto, en el ámbito del SGSI presentado en el presente documento, al igual que para la evaluación de riesgos, esta gestión de riesgos ya ha sido realizada.

5.8.1.6 Evaluación del funcionamiento

- Monitorización, medida, análisis y evaluación: Llegados a este punto, es posible afirmar que la organización está monitorizando el funcionamiento del SGSI definido en el presente documento.
- Auditorías Internas: La implantación del SGSI no implica una mejora que incorpore un nivel de madurez adicional al presente requerimiento.
- Revisión por parte de la Dirección: Al amparo del presente SGSI se ha definido un procedimiento de revisión por parte de la Dirección. Dicho procedimiento queda detallado en el documento “MuñozMercaderEDGAR_TFM_Procedimiento Revision por Direccion v1.1” adjunto.

5.8.1.7 Mejora continua

- No-conformidades y Acciones Correctoras: Existe consciencia de que surgirán no-conformidades y de que se deberán aplicar acciones correctoras, pero en esta fase del SGSI en la que se está en la primera iteración de la mejora continua, aún no se ha dado el caso.
- Mejora continua: Existe consciencia de que la implantación de un SGSI es un proceso de mejora continua, pero en la fase actual, en la que se está en una primera iteración, aún no existe documentación asociada.

Siguiendo los mismos criterios utilizados en el punto 1.3.1 la tabla resultante es la se detalla a continuación. Se ha destacado en color verde aquellos requerimientos que tras la implantación del SGSI su nivel de madurez ha mejorado.

Requisitos	**Requisito promedio**	**Sub-requisitos**				
Contexto de la Organización	3,5	3	4	4	3	
Liderazgo	4,0	4	4	4		
Planificación	4,0	4	4			
Soporte	3,6	3	3	4	4	4
Operación	2,7	2	4	2		
Evaluación del funcionamiento	3,0	2	4	3		
Mejora continua	1,0	1	1			

Tabla 15: Cumplimiento requisitos ISO/IEC 27001

A continuación se muestra la distribución en el grado de madurez de los diferentes requerimientos según el anterior detalle.

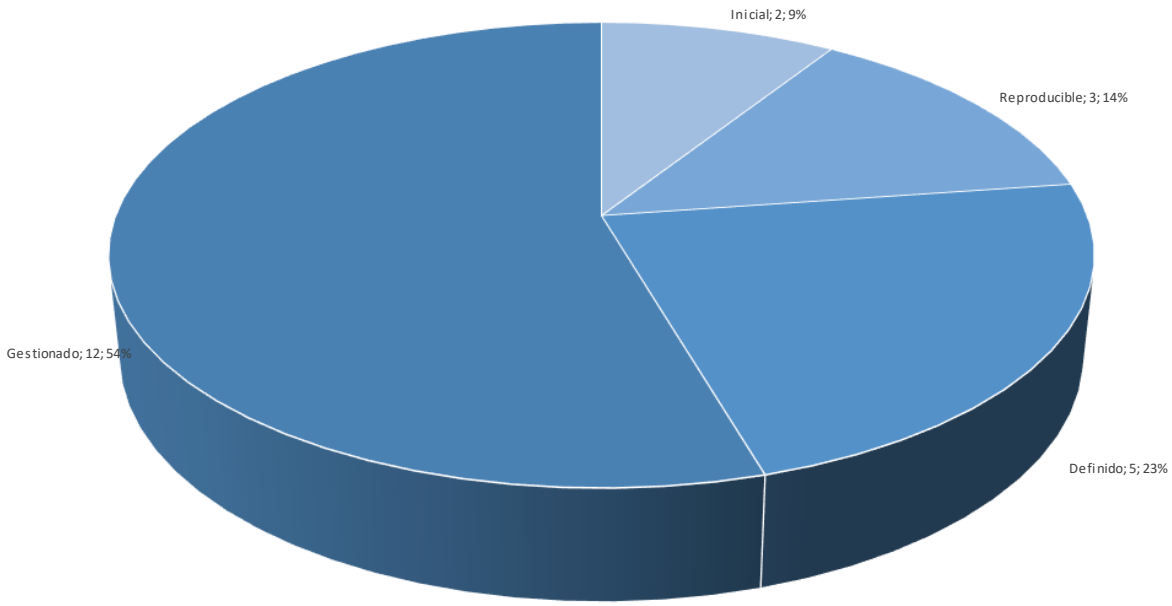


Imagen 23: Requerimientos ISO/IEC 27001 - Distribución según el grado de madurez

La evolución en la distribución del grado de madurez se puede observar comparando el anterior gráfico con el obtenido tras el análisis de la situación inicial (punto 1.3.1).

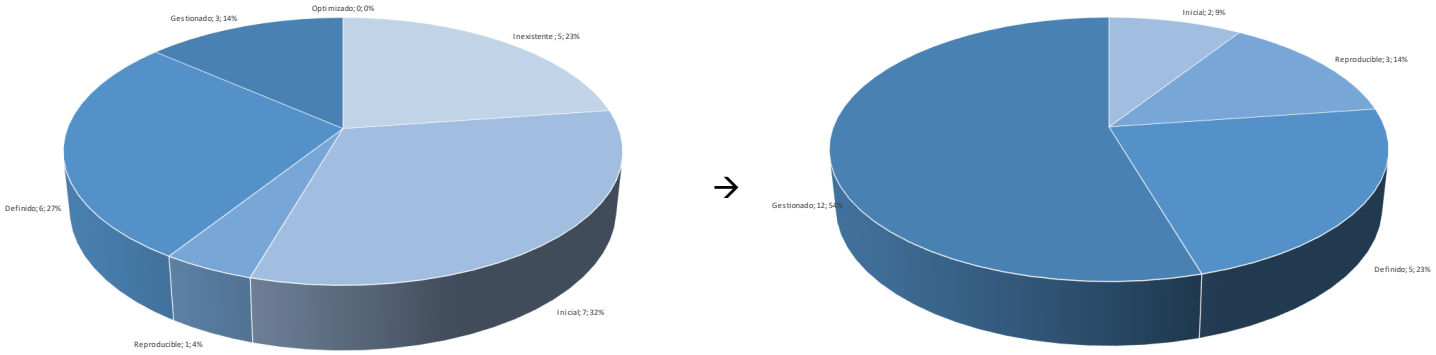


Imagen 24: Requerimientos ISO/IEC 27001 – Evolución del grado de madurez

A continuación se muestra gráficamente el estado de madurez en los requisitos planteados por la ISO/IEC 27001 de Integrador X tras la implantación de los proyectos de mejora expuestos en el punto 4. Para facilitar la comparación se mostrará también la situación previa a la implementación de los proyectos de mejora (representación mostrada en la Imagen 5).

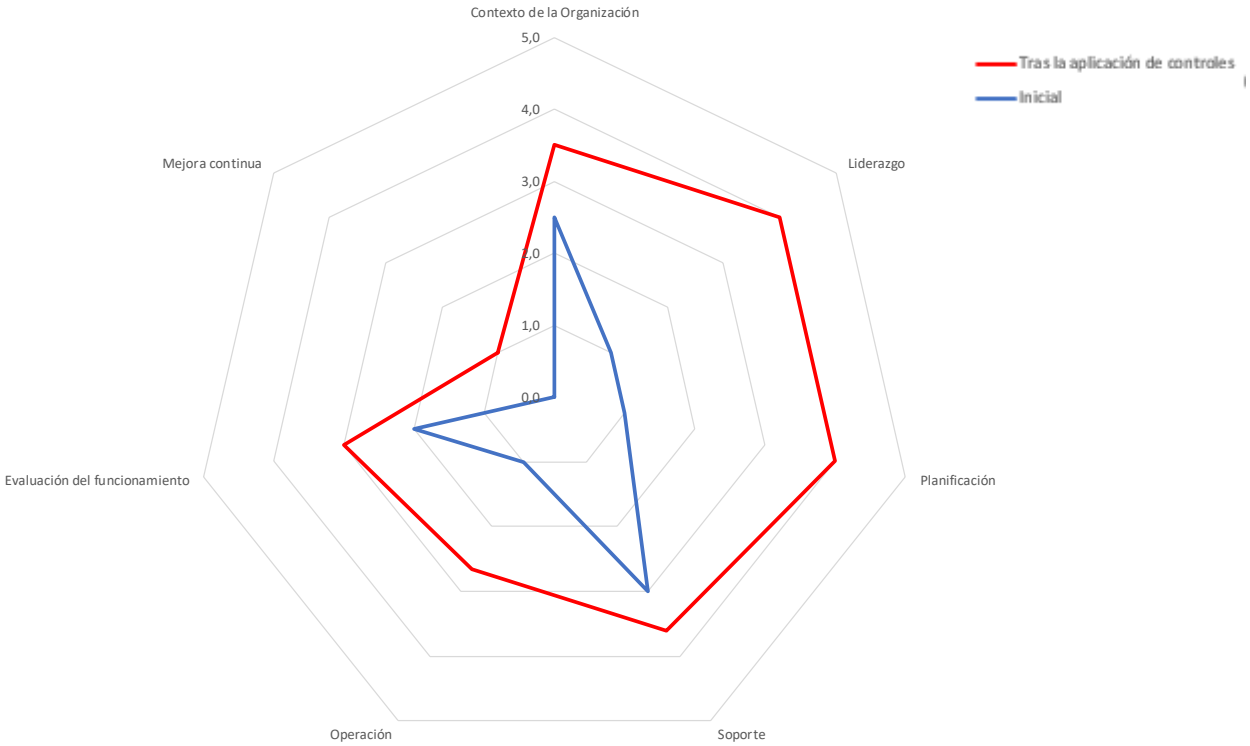


Imagen 25: Grado de madurez de los requisitos de la ISO/IEC 27001

5.8.2 Controles ISO/IEC 27002

A parte de los requerimientos definidos en la ISO/IEC 27001, la ISO/IEC 27002:2013 establece 14 dominios con un total de 35 categorías principales. A su vez, para cada una de estas 35 categorías de control se especifican el/los objetivo/s de control y una o más acciones para conseguir dicho objetivo (control/es), en total la ISO/IEC 27002:2013 define 114 controles.

En el caso de Integrador X la evolución en el ámbito de la Seguridad de la Información, en relación con los controles definidos en la ISO/IEC 27002:2013, tras la implantación de SGSI detallado en el presente documento, es la detallada a continuación[11]:

5. Políticas de seguridad de la información

5.1. Directrices de la Dirección en seguridad de la información:

5.1.1. Políticas para la seguridad de la información: La implantación del presente SGSI implícita la definición de las pertinentes Políticas de Seguridad de la Información

[11] En el caso de no comentarse nada explícitamente para una Categoría o un Control, para esta Categoría o Control aplica el comentario jerárquicamente superior, del Capítulo o Categoría, respectivamente.

definidas en el documento anexo "MuñozMercaderEDGAR_TFM_Politica_Seguridad de la Informacion v1.1".

5.1.2. Revisión de las políticas para la seguridad de la información: La implantación del presente SGSI implícita la definición del pertinente protocolo de revisión de dichas políticas. Existe un procedimiento para la revisión de éstas por parte de la dirección: "MuñozMercaderEDGAR_TFM_Procedimiento Revision por Direccion v1.1".

6. **Organización de la seguridad de la información**
   - 6.1. **Organización Interna:** La implantación del SGSI no implica una mejora en la presente categoría salvo los casos indicados explícitamente.
     - 6.1.1. Roles y responsabilidades en Seguridad de la Información: Al amparo del presente SGSI se definen los diferentes roles y responsabilidades definidos en el documento adjunto "MuñozMercaderEDGAR_TFM_Roles y Responsabilidades v1.1".
     - 6.1.2. Segregación de tareas
     - 6.1.3. Contacto con las autoridades
     - 6.1.4. Contacto con grupos de interés especial
     - 6.1.5. Seguridad de la Información en la gestión de proyectos
   - 6.2. **Los dispositivos móviles y el teletrabajo:** La implantación del SGSI no implica una mejora en la presente categoría.
     - 6.2.1. Política de dispositivos móviles
     - 6.2.2. Teletrabajo
7. **Seguridad relativa a los recursos humanos:** La implantación del SGSI no implica una mejora en el presente dominio.
   - 7.1. **Antes del empleo**
     - 7.1.1. Investigación de antecedentes
     - 7.1.2. Términos y condiciones del empleo
   - 7.2. **Durante el empleo**
     - 7.2.1. Responsabilidades de gestión
     - 7.2.2. Concienciación, educación y capacitación en seguridad de la información
     - 7.2.3. Proceso disciplinario
   - 7.3. **Finalización del empleo o cambio de puesto de trabajo**
     - 7.3.1. Responsabilidades ante una finalización o cambio
8. **Gestión de activos**
   - 8.1. **Responsabilidad sobre los activos:**
     - 8.1.1. Inventario de activos: A raíz de la elaboración del análisis de riesgos se dispone de una primera versión de un inventario de activos.
     - 8.1.2. Propiedad de los activos: Relacionado con el anterior punto, la elaboración del análisis de riesgos ha implicado la valoración de los diferentes activos implicados. Esta ha sido realizada por sus propietarios.
     - 8.1.3. Uso aceptable de los activos: Al igual que en el anterior caso la definición del uso aceptable de los activos ha sido realizada por sus propietarios.
     - 8.1.4. Devolución de activos: La implantación del SGSI no implica una mejora en el presente control.
   - 8.2. **Clasificación de la información:** Al amparo del proyecto de mejora "Implementación de un sistema DLP (Data Loss Prevention)" se ha llevado a cabo todo un proceso de Clasificación, Etiquetado y definición de Manipulación de la información.
     - 8.2.1. Clasificación de la información
     - 8.2.2. Etiquetado de la información
     - 8.2.3. Manipulado de la información

8.3. **Manipulación de soportes:** La implantación del SGSI no implica una mejora en la presente categoría.
8.3.1. Gestión de soportes extraíbles
8.3.2. Eliminación de soportes
8.3.3. Soportes físicos en tránsito

9. **Control de acceso**
9.1. **Requisitos de negocio para el control de acceso:** La implantación del SGSI no implica una mejora en la presente categoría.
9.1.1. Política de control de acceso
9.1.2. Acceso a las redes y a los servicios de red
9.2. **Gestión de acceso de usuario**
9.2.1. Registro y baja de usuario: La implantación del SGSI no implica una mejora en el presente control.
9.2.2. Provisión de acceso de usuario: La implantación del SGSI no implica una mejora en el presente control.
9.2.3. Gestión de privilegios de acceso: A raíz de la implantación del SGSI se toma conciencia de la necesidad de gestionar los privilegios de acceso en función del rol de cada empleado.
9.2.4. Gestión de la información secreta de autenticación de los usuarios: A raíz de la implantación del proyecto de mejora "Implementación de un sistema de autenticación de doble factor" se incrementa sustancialmente la fiabilidad en la autenticación de los usuarios.
9.2.5. Revisión de los derechos de acceso de usuario: A raíz de la implantación del SGSI se toma conciencia de la necesidad de gestionar los privilegios de acceso en función del rol de cada empleado.
9.2.6. Retirada o reasignación de los derechos de acceso: A raíz de la implantación del SGSI se toma conciencia de la necesidad de gestionar los privilegios de acceso en función del rol de cada empleado.
9.3. **Responsabilidades del usuario:** La implantación del SGSI no implica una mejora en la presente categoría.
9.3.1. Uso de la información secreta de autenticación
9.4. **Control de acceso a sistemas y aplicaciones:**
9.4.1. Restricción del acceso a la información: La implantación del SGSI no implica una mejora en el presente control.
9.4.2. Proceso seguro de inicio de sesión: La implantación del SGSI no implica una mejora en el presente control.
9.4.3. Sistema de gestión de contraseñas: A raíz de la implantación del proyecto de mejora "Implementación de un sistema de autenticación de doble factor" se incrementa sustancialmente la fiabilidad en la autenticación de los usuarios.
9.4.4. Uso de utilidades con privilegios del sistema: La implantación del SGSI no implica una mejora en el presente control.
9.4.5. Control de acceso al código fuente de los programas: A raíz de la implantación del proyecto de mejora "Implementación de un sistema de autenticación de doble factor" se incrementa sustancialmente la fiabilidad en la autenticación de los usuarios.

10. **Criptografía**
10.1. **Controles criptográficos**
10.1.1. Política de uso de los controles criptográficos: Al existir ya una política al respecto, la implantación del SGSI no implica una mejora en el presente control.
10.1.2. Gestión de claves: A raíz de la implantación del proyecto de mejora "Implementación de un sistema criptográfico corporativo de clave pública (PKI)"

se dispone de las herramientas necesarias para la realización de una gestión de claves adecuada alineada con los requerimientos de seguridad de la organización.

11. **Seguridad física y del entorno:** La implantación del SGSI no implica una mejora en el presente dominio.
    - 11.1. **Áreas seguras**
        - 11.1.1. Perímetro de seguridad física
        - 11.1.2. Controles físicos de entrada
        - 11.1.3. Seguridad de oficinas, despachos y recursos
        - 11.1.4. Protección contra amenazas externas y ambientales
        - 11.1.5. El trabajo en áreas seguras
        - 11.1.6. Áreas de carga y descarga
    - 11.2. **Seguridad de los equipos**
        - 11.2.1. Emplazamiento y protección de equipos
        - 11.2.2. Instalaciones de suministro
        - 11.2.3. Seguridad de cableado
        - 11.2.4. Mantenimiento de equipos
        - 11.2.5. Retirada de materiales propiedad de la empresa
        - 11.2.6. Seguridad de los equipos fuera de las instalaciones
        - 11.2.7. Reutilización o eliminación segura de equipos
        - 11.2.8. Equipo de usuario desatendido
        - 11.2.9. Política de puesto de trabajo despejado y pantalla limpia
12. **Seguridad de las operaciones**
    - 12.1. **Procedimientos y responsabilidades operacionales:** La implantación del SGSI no implica una mejora en el presente control por estar este ya en un nivel de madurez máximo.
        - 12.1.1. Documentación de procedimientos de la operación
        - 12.1.2. Gestión de cambios
        - 12.1.3. Gestión de capacidades
        - 12.1.4. Separación de los recursos de desarrollo, pruebas y operación
    - 12.2. **Protección contra el software malicioso**
        - 12.2.1. Controles contra el código malicioso: El proyecto de mejora “Implantación de sistemas Antimalware, ZeroDay, anti-APT” incrementa el nivel de madurez de este control al ser actualizada la protección de la organización según las nuevas amenazas existentes.
    - 12.3. **Copias de seguridad:**
        - 12.3.1. Copias de Seguridad de la Información: El proyecto de mejora “Implementación de un sistema de backup de la información en cloud” aporta mejoras adicionales al presente control.
    - 12.4. **Registros y supervisión:** La implantación del SGSI no implica una mejora en la presente categoría.
        - 12.4.1. Registro de eventos
        - 12.4.2. Protección de la información de registro
        - 12.4.3. Registros de administración y operación
        - 12.4.4. Sincronización del reloj
    - 12.5. **Control del software en explotación:** La implantación del SGSI no implica una mejora en la presente categoría.
        - 12.5.1. Instalación del software en explotación
    - 12.6. **Gestión de vulnerabilidades técnicas:**

12.6.1. Gestión de las vulnerabilidades técnicas: El proyecto de mejora “Implantación de sistemas Antimalware, ZeroDay, anti-APT” aporta cierto grado de protección ante las vulnerabilidades técnicas de los equipos.
12.6.2. Restricción en la instalación de software: La implantación del SGSI no implica una mejora en el presente control.
12.7. **Consideraciones sobre la auditoría de Sistemas de Información:** La implantación del SGSI no implica una mejora en la presente categoría.
12.7.1. Controles de auditoría de sistemas operativos
13. **Seguridad de las comunicaciones**
13.1. **Gestión de la seguridad de redes:** Salvo en el caso en el que se indica lo contrario, la implantación del SGSI no implica una mejora en la presente categoría.
13.1.1. Controles de red
13.1.2. Seguridad de los servicios de red: El proyecto de mejora “Implementación de redundancia / alta disponibilidad en las comunicaciones corporativas” incorpora un incremento en el nivel de madurez del presente control.
13.1.3. Segregación en redes
13.2. **Intercambio de información:** La implantación del SGSI no implica una mejora en la presente categoría.
13.2.1. Políticas y procedimientos de intercambio de información
13.2.2. Acuerdos de intercambio de información
13.2.3. Mensajería electrónica
13.2.4. Acuerdos de confidencialidad o no revelación
14. **Adquisición, desarrollo y mantenimiento de los sistemas de información**
14.1. **Requisitos de seguridad en sistemas de información:** A raíz de la implantación del SGSI descrito en el presente documento, Integrador X incorpora un grado de madurez adicional a la presente categoría de control.
14.1.1. Análisis de requisitos y especificaciones de seguridad de la información
14.1.2. Asegurar los servicios de aplicaciones en redes públicas
14.1.3. Protección de las transacciones de servicios de aplicaciones
14.2. **Seguridad en el desarrollo y en los procesos de soporte:** La implantación del SGSI no implica una mejora en el presente control por estar este ya en un nivel de madurez máximo.
14.2.1. Política de desarrollo seguro
14.2.2. Procedimiento de control de cambios en sistemas
14.2.3. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
14.2.4. Restricciones a los cambios en los paquetes de software
14.2.5. Principios de ingeniería de sistemas seguros
14.2.6. Entorno de desarrollo seguro
14.2.7. Externalización del desarrollo de software
14.2.8. Pruebas funcionales de seguridad de sistemas
14.2.9. Pruebas de aceptación de sistemas
14.3. **Datos de prueba:** La implantación del SGSI no implica una mejora en la presente categoría.
14.3.1. Protección de los datos de prueba
15. **Relación con proveedores:** La implantación del SGSI no implica una mejora en el presente dominio.
15.1. **Seguridad en las relaciones con proveedores:**
15.1.1. Política de seguridad de la información en las relaciones con los proveedores
15.1.2. Requisitos de seguridad en contratos con terceros
15.1.3. Cadena de suministro de tecnología de la información u de las comunicaciones

- **15.2. Gestión de la provisión de servicios del proveedor:**
  - 15.2.1. Control y revisión de la provisión de servicios del proveedor
  - 15.2.2. Gestión de cambios en la provisión del servicio del proveedor
- **16. Gestión de incidentes de seguridad de la información:** La implantación del SGSI no implica una mejora en el presente dominio.
  - **16.1. Gestión de incidentes de seguridad de la información y mejoras:**
    - 16.1.1. Responsabilidades y procedimientos
    - 16.1.2. Notificación de los eventos de seguridad de la información
    - 16.1.3. Notificación de puntos débiles de la seguridad
    - 16.1.4. Evaluación y decisión sobre los eventos de seguridad de información
    - 16.1.5. Respuesta a incidentes de seguridad de la información
    - 16.1.6. Aprendizaje de los incidentes de seguridad de la información
    - 16.1.7. Recopilación de evidencias
- **17. Aspectos de seguridad de la información para la gestión de la continuidad del negocio:** Los proyectos de mejora "Contratación de los Servicios de un CPD de respaldo ", "Implementación de redundancia / alta disponibilidad en las comunicaciones corporativas", "Implantación de un sistema de Anti-DDoS" y "Implementación de un sistema de backup de la información en cloud" añaden madurez en general al presente dominio.
  - **17.1. Continuidad de la seguridad de la información**
    - 17.1.1. Planificación de la continuidad de la seguridad de la información: El plan de proyectos definido establece una ruta para la mejora en la continuidad de la seguridad de la información.
    - 17.1.2. Implementar la continuidad de la seguridad de la información: Los proyectos enunciados anteriormente incrementan el nivel de madurez del presente control.
    - 17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información: La implantación de los anteriores proyectos implica implícitamente una mejora en el presente control.
  - **17.2. Redundancias**
    - 17.2.1. Disponibilidad de los recursos de tratamiento de la información: Los proyectos enunciados anteriormente incrementan el nivel de madurez del presente control.
- **18. Cumplimiento:** La implantación del SGSI no implica una mejora en el presente dominio.
  - **18.1. Cumplimiento de los requisitos legales y contractuales:**
    - 18.1.1. Identificación de la legislación aplicable y de los requisitos contractuales
    - 18.1.2. Derechos de propiedad intelectual (DPI)
    - 18.1.3. Protección de los registros de la organización
    - 18.1.4. Protección y privacidad de la información de carácter personal
    - 18.1.5. Regulación de los controles criptográficos
  - **18.2. Revisiones de la seguridad de la información:**
    - 18.2.1. Revisión independiente de la seguridad de la información
    - 18.2.2. Cumplimiento de las políticas y normas de seguridad
    - 18.2.3. Comprobación del cumplimiento técnico

A continuación se muestra la distribución en el grado de madurez de los diferentes controles según el anterior detalle.

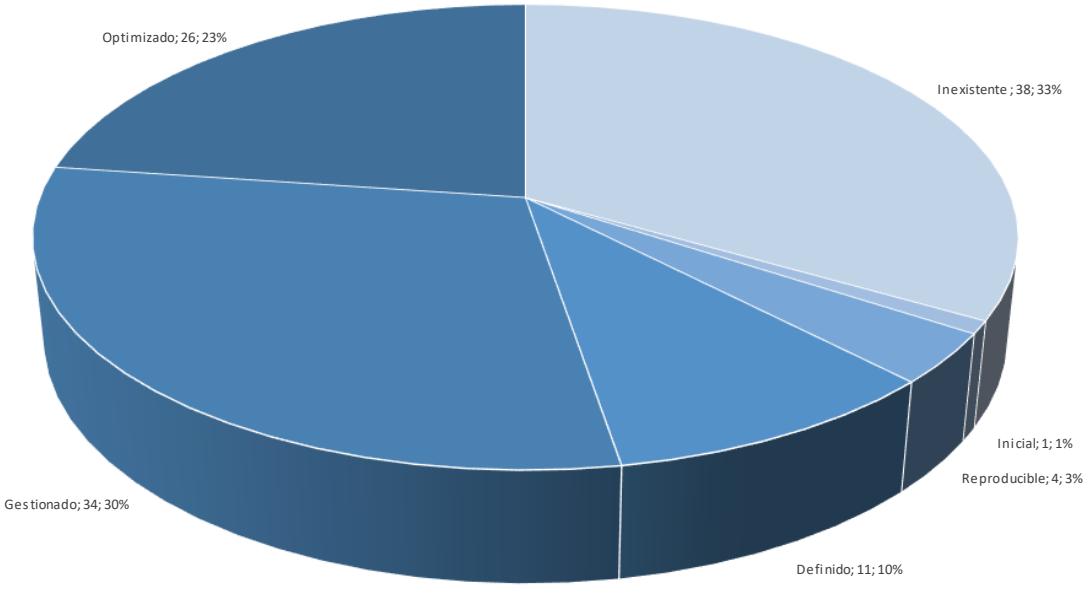


Imagen 26 Controles ISO/IEC 27002 - Distribución según el grado de madurez

La evolución en la distribución del grado de madurez se puede observar comparando el anterior gráfico con el obtenido tras el análisis de la situación inicial.

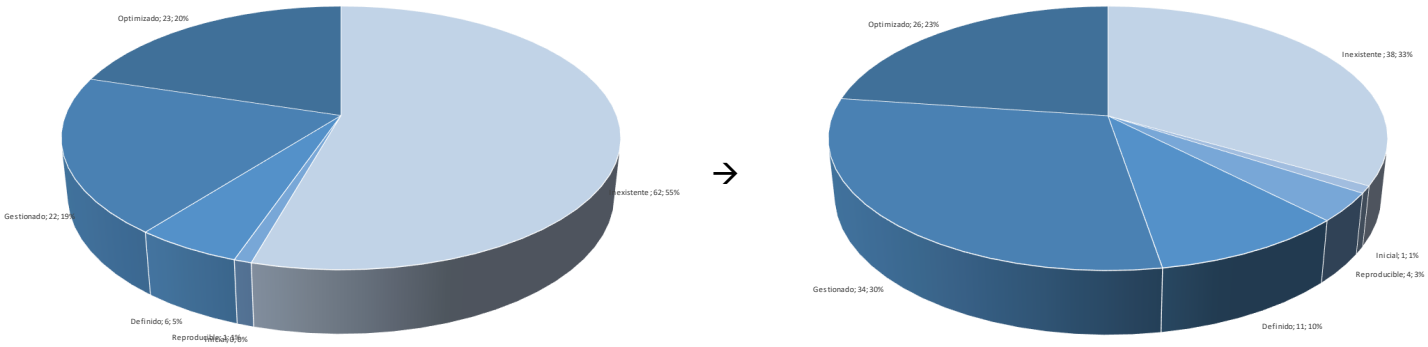


Imagen 27: Controles ISO/IEC 27002 – Evolución del grado de madurez

A continuación se muestra gráficamente el estado de madurez en cada uno de los dominios definidos en la ISO/IEC 27002 de Integrador X tras la implantación de los proyectos de mejora expuestos en el punto 4.

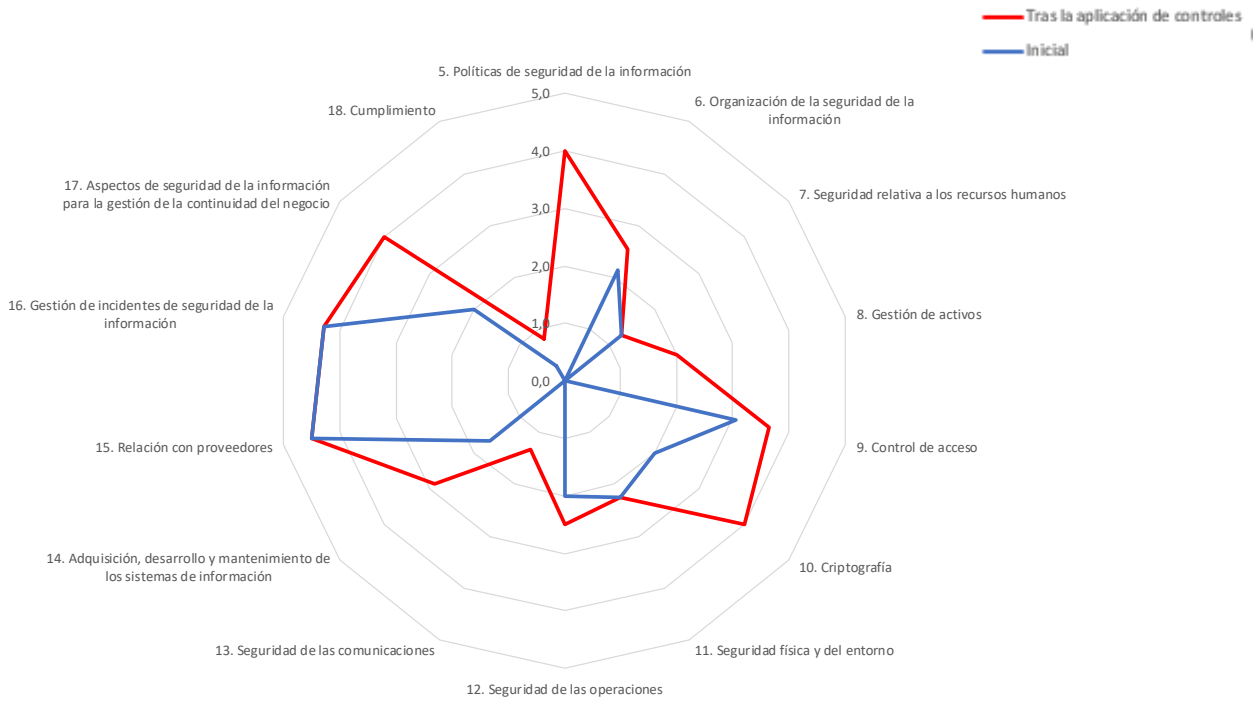


Imagen 28: Grado de madurez de los dominios de la ISO/IEC 27002

Como se puede observar en la anterior gráfica existen dominios en los que no se ha producido mejora tras la aplicación de los proyectos de mejora planteados. Esto es debido a que, para estos dominios, tras el análisis de riesgos, no se ha considerado necesario la mejora en su seguridad por no presentar un riesgo por encima del umbral aceptado por la organización y por tanto los proyectos planteados no han pretendido una mejora en dicho sentido.

5.9 Planes de Mejora Propuestos

Existen ciertos indicadores definidos en “MuñozMercaderEDGAR_TFM_Gestion de Indicadores v1.1.pdf” que no han podido ser evaluados en la presente auditoría por falta de mecanismos para su medida. Deberá evaluarse la utilidad de dichos indicadores y en el caso de considerarse de aplicación, deberán definirse los mecanismos de medida pertinentes.

De manera genérica, como Plan de Mejora futuro del SGSI se proponer la mejora del estado de madurez de los diferentes requerimientos y controles definidos en las ISO/IEC 27001 e ISO/IEC 27002, respectivamente, priorizando aquellos con un menor nivel de madurez. Es decir, la prioridad a la hora de potenciar la mejora del estado de madurez de los requerimientos definidos en la ISO/IEC 27001 debería ser:

1. Mejora continua
2. Operación

3. Evaluación del funcionamiento
4. Contexto de la Organización
5. Soporte
6. Liderazgo y Planificación al mismo nivel.

Y la prioridad a la hora de potenciar la mejora del estado de madurez de los controles definidos en la ISO/IEC 27002 debería ser[12]:

1. 13. Seguridad de las comunicaciones
2. 7. Seguridad relativa a los recursos humanos
3. 8. Gestión de activos
4. 12. Seguridad de las operaciones
5. 6. Organización de la seguridad de la información
6. 14. Adquisición, desarrollo y mantenimiento de los sistemas de información
7. 9. Control de acceso
8. 5. Políticas de seguridad de la información
9. 10. Criptografía
10. 17. Aspectos de seguridad de la información para la gestión de la continuidad del negocio
11. 16. Gestión de incidentes de seguridad de la información
12. 15. Relación con proveedores

Por otro lado deberá hacerse hincapié en aquellos proyectos de mejora que aún no han sido completamente desplegados debiendo revisar en futuras auditorías su grado de avance con respecto a su situación anterior.

5.10 Problemas encontrados en el desarrollo de la auditoría

Existen ciertos indicadores definidos en “MuñozMercaderEDGAR_TFM_Gestion de Indicadores v1.1.pdf” que no han podido ser evaluados en la presente auditoría por falta de mecanismos para su medida. Deberá evaluarse la utilidad de dichos indicadores y en el caso de considerarse de aplicación, deberán definirse los mecanismos de medida pertinentes.

No se han identificado más problemas a lo largo del desarrollo de la presente auditoria.

[12] Los dominios: 18. Cumplimiento y 11. Seguridad física y del entorno, no se han incluido en el anterior listado por no ser de aplicabilidad en el SGSI según queda reflejado en la Declaración de Aplicabilidad detallada en el documento anexo “MuñozMercaderEDGAR_TFM_Declaracion de Aplicabilidad v1.1”.

6. ANEXOS

6.1 Detalle de Amenazas

A continuación se detallan, para cada categoría de activo, las amenazas identificadas con su correspondiente probabilidad de ocurrencia y afectación para cada una de las dimensiones.

Amenaza	Probabilidad (días/año)	Probabilidad	Degradación				
			A	C	I	D	T
Instalaciones							
[N.1] Fuego	0,05	0,01%				20%	
[N.2] Daños por agua	0,00	0,00%				5%	
[N.*] Desastres naturales	0,01	0,00%				80%	
[I.1] Fuego	0,10	0,03%				20%	
[I.2] Daños por agua	1,00	0,27%				5%	
[I.*] Desastres industriales	1,00	0,27%				0%	
[I.11] Emanaciones electromagnéticas	0,00	0,01%		80%			
[E.15] Alteración accidental de la información	5,00	1,37%			1%		
[E.18] Destrucción de información	5,00	1,37%				1%	
E.19] Fugas de información	5,00	1,37%		1%			
[A.7] Uso no previsto	100,00	27,40%		0%	0%	0%	
[A.11] Acceso no autorizado	10,00	2,74%		1%	1%		
[A.15] Modificación deliberada de la información	0,10	0,03%			50%		
[A.18] Destrucción de información	0,10	0,03%				1%	
[A.19] Divulgación de información	1,00	0,27%		50%			
[A.26] Ataque destructivo	0,03	0,01%				20%	
[A.27] Ocupación enemiga	0,00	0,00%		50%		50%	
Hardware							
[N.1] Fuego	0,05	0,01%				20%	
[N.2] Daños por agua	0,00	0,00%				5%	
[N.*] Desastres naturales	0,01	0,00%				80%	
[I.1] Fuego	0,10	0,03%				50%	
[I.2] Daños por agua	1,00	0,27%				10%	
[I.*] Desastres industriales	1,00	0,27%				0%	
[I.3] Contaminación mecánica	1,00	0,27%				1%	
[I.4] Contaminación electromagnética	10,00	2,74%				1%	
[I.5] Avería de origen físico o lógico	100,00	27,40%				5%	
[I.6] Corte del suministro eléctrico	1,00	0,27%				1%	
[I.7] Condiciones inadecuadas de temperatura o humedad	1,00	0,27%				1%	

[I.11] Emanaciones electromagnéticas	0,00	0,01%		80%			
[E.2] Errores del administrador	4,00	1,10%		20%	20%	20%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1,00	0,27%		20%	20%	20%	
[E.24] Caída del sistema por agotamiento de recursos	0,33	0,09%				80%	
[E.25] Pérdida de equipos	5,00	1,37%		50%		10%	
[A.6] Abuso de privilegios de acceso	10,00	2,74%		1%	1%	1%	
[A.7] Uso no previsto	100,00	27,40%		1%	1%	1%	
[A.11] Acceso no autorizado	0,33	0,09%		50%	50%		
[A.23] Manipulación de los equipos	0,33	0,09%		50%		80%	
[A.24] Denegación de servicio	0,33	0,09%				80%	
[A.25] Robo	5,00	1,37%		50%		10%	
[A.26] Ataque destructivo	0,10	0,03%				50%	
Aplicaciones							
[I.5] Avería de origen físico o lógico	2,00	0,55%				5%	
[E.1] Errores de los usuarios	20,00	5,48%		5%	5%	5%	
[E.2] Errores del administrador	4,00	1,10%		20%	20%	20%	
[E.8] Difusión de software dañino	1,00	0,27%		80%	80%	80%	
[E.9] Errores de [re-]encaminamiento	1,00	0,27%		10%			
[E.10] Errores de secuencia	5,00	1,37%			5%		
[E.15] Alteración accidental de la información	10,00	2,74%			5%		
[E.18] Destrucción de información	10,00	2,74%				20%	
[E.19] Fugas de información	5,00	1,37%		5%			
[E.20] Vulnerabilidades de los programas (software)	5,00	1,37%		5%	5%	5%	
[E.21] Errores de mantenimiento / actualización de programas (software)	10,00	2,74%		1%	1%	1%	
[A.5] Suplantación de la identidad del usuario	1,00	0,27%	80%	80%	50%		
[A.6] Abuso de privilegios de acceso	10,00	2,74%		1%	1%	1%	
[A.7] Uso no previsto	100,00	27,40%		1%	1%	1%	
[A.8] Difusión de software dañino	1,00	0,27%		50%	50%	80%	
[A.9] [Re-]encaminamiento de mensajes	0,33	0,09%		80%			
[A.10] Alteración de secuencia	0,33	0,09%			50%		
[A.11] Acceso no autorizado	1,00	0,27%		50%	50%		
[A.15] Modificación deliberada de la información	0,33	0,09%			80%		
[A.18] Destrucción de información	0,33	0,09%				80%	

[A.19] Divulgación de información	0,33	0,09%		80%			
[A.22] Manipulación de programas	0,10	0,03%		80%	80%	80%	
Datos/Información							
[E.1] Errores de los usuarios	20,00	5,48%		10%	10%	10%	
[E.2] Errores del administrador	4,00	1,10%		20%	20%	20%	
[E.15] Alteración accidental de la información	10,00	2,74%			5%		
[E.18] Destrucción de información	10,00	2,74%				30%	
[E.19] Fugas de información	5,00	1,37%		10%			
[A.5] Suplantación de la identidad del usuario	1,00	0,27%	80%	80%	50%		
[A.6] Abuso de privilegios de acceso	10,00	2,74%		5%	5%	5%	
[A.11] Acceso no autorizado	1,00	0,27%		60%	60%		
[A.15] Modificación deliberada de la información	0,33	0,09%			80%		
[A.18] Destrucción de información	0,33	0,09%				80%	
[A.19] Divulgación de información	0,33	0,09%		80%			
Redes de Comunicaciones							
[I.8] Fallo de servicios de comunicaciones	1,00	0,27%		80%			
[E.2] Errores del administrador	4,00	1,10%		10%	5%	50%	
[E.9] Errores de [re-]encaminamiento	1,00	0,27%		10%			
[E.10] Errores de secuencia	0,20	0,05%			0%		
[E.15] Alteración accidental de la información	0,20	0,05%			0%		
[E.18] Destrucción de información	0,20	0,05%				30%	
[E.19] Fugas de información	0,10	0,03%		0%			
[E.24] Caída del sistema por agotamiento de recursos	0,33	0,09%				80%	
[A.5] Suplantación de la identidad del usuario	1,00	0,27%	80%	80%	50%		
[A.6] Abuso de privilegios de acceso	10,00	2,74%		1%	1%	1%	
[A.7] Uso no previsto	100,00	27,40%		1%	1%	1%	
[A.9] [Re-]encaminamiento de mensajes	0,33	0,09%		80%			
[A.10] Alteración de secuencia	0,33	0,09%			50%		
[A.11] Acceso no autorizado	1,00	0,27%		50%	50%		
[A.12] Análisis de tráfico	0,33	0,09%		50%			
[A.14] Interceptación de información (escucha)	0,20	0,05%		80%			
[A.15] Modificación deliberada de la información	0,33	0,09%			80%		
[A.19] Divulgación de información	0,33	0,09%		80%			

[A.24] Denegación de servicio	0,33	0,09%				80%	
Servicios/Servicios Auxiliares							
[E.1] Errores de los usuarios	20,00	5,48%		5%	5%	5%	
[E.2] Errores del administrador	4,00	1,10%		20%	20%	20%	
[E.9] Errores de [re-]encaminamiento	1,00	0,27%		10%			
[E.10] Errores de secuencia	5,00	1,37%			5%		
[E.15] Alteración accidental de la información	10,00	2,74%			5%		
[E.18] Destrucción de información	10,00	2,74%				20%	
[E.19] Fugas de información	5,00	1,37%		5%			
[E.20] Vulnerabilidades de los programas (software)	5,00	1,37%		5%	5%	5%	
[E.24] Caída del sistema por agotamiento de recursos	0,10	0,03%				80%	
[A.5] Suplantación de la identidad del usuario	1,00	0,27%	80%	80%	50%		
[A.6] Abuso de privilegios de acceso	5,00	1,37%		1%	1%	1%	
[A.7] Uso no previsto	50,00	13,70%		1%	1%	1%	
[A.9] [Re-]encaminamiento de mensajes	0,33	0,09%		80%			
[A.10] Alteración de secuencia	0,33	0,09%			50%		
[A.11] Acceso no autorizado	1,00	0,27%		50%	50%		
[A.13] Repudio	3,00	0,82%					10%
[A.15] Modificación deliberada de la información	0,33	0,09%			80%		
[A.18] Destrucción de información	0,33	0,09%				80%	
[A.19] Divulgación de información	0,33	0,09%		80%			
[A.24] Denegación de servicio	0,33	0,09%				80%	
Equipamiento Auxiliar							
[N.1] Fuego	0,05	0,01%				2%	
[N.2] Daños por agua	0,00	0,00%				1%	
[N.*] Desastres naturales	0,01	0,00%				8%	
[I.1] Fuego	0,10	0,03%				5%	
[I.2] Daños por agua	1,00	0,27%				1%	
[I.*] Desastres industriales	1,00	0,27%				0%	
[I.3] Contaminación mecánica	1,00	0,27%				0%	
[I.4] Contaminación electromagnética	10,00	2,74%				0%	
[I.5] Avería de origen físico o lógico	100,00	27,40%				1%	
[I.6] Corte del suministro eléctrico	1,00	0,27%				0%	
[I.7] Condiciones inadecuadas de temperatura o humedad	1,00	0,27%				0%	
[I.9] Interrupción de otros servicios y suministros esenciales	1,00	0,27%				0%	

[I.10] Degradación de los soportes de almacenamiento de la información	0,20	0,05%				20%	
[I.11] Emanaciones electromagnéticas	0,00	0,00%		16%			
[E.1] Errores de los usuarios	20,00	5,48%		1%	1%	1%	
[E.2] Errores del administrador	4,00	1,10%		4%	4%	4%	
[E.15] Alteración accidental de la información	10,00	2,74%			1%		
[E.18] Destrucción de información	10,00	2,74%				2%	
[E.19] Fugas de información	5,00	1,37%		5%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,00	0,00%		4%	4%	2%	
[E.25] Pérdida de equipos	5,00	1,37%		10%		1%	
[A.7] Uso no previsto	100,00	27,40%		0%	0%	0%	
[A.11] Acceso no autorizado	0,33	0,09%		10%	10%		
[A.15] Modificación deliberada de la información	0,33	0,09%			16%		
[A.18] Destrucción de información	0,33	0,09%				8%	
[A.19] Divulgación de información	0,33	0,09%		16%			
[A.23] Manipulación de los equipos	0,33	0,09%		10%		8%	
[A.25] Robo	5,00	1,37%		10%		1%	
[A.26] Ataque destructivo	0,10	0,03%				5%	
Personal							
[E.7] Deficiencias en la organización	4,00	1,10%				30%	
[E.19] Fugas de información	10,00	2,74%		10%			
[E.28] Indisponibilidad del personal	10,00	2,74%				30%	
[A.28] Indisponibilidad del personal	2,00	0,55%				30%	
[A.29] Extorsión	0,20	0,05%		50%	50%	50%	
[A.30] Ingeniería social (picaresca)	1,00	0,27%		30%	30%	30%	

Tabla 16: Detalle de Amenazas

6.2 Detalle de Impactos

Categoría	Activo	Categoría superior	Valor	Dimensiones					Amenaza	Probabilidad	Degradación				Impacto				Impacto
				A	C	I	D	T			A	C	I	D	T	A	C	I	D	T	
Activos Esenciales	[S] Servicios de Ejecución de F	-	A	1	7	5	6	1	[E.1] Errores de los usuarios	5,48%		5%	5%	5%		0,00	0,35	0,25	0,30	0,00	**0,35**
									[E.2] Errores del administrador	1,10%		20%	20%	20%		0,00	1,40	1,00	1,20	0,00	**1,40**
									[E.9] Errores de [re-]encaminamier	0,27%		10%				0,00	0,70	0,00	0,00	0,00	**0,70**
									[E.10] Errores de secuencia	1,37%			5%			0,00	0,00	0,25	0,00	0,00	**0,25**
									[E.15] Alteración accidental de la ir	2,74%			5%			0,00	0,00	0,25	0,00	0,00	**0,25**
									[E.18] Destrucción de información	2,74%				20%		0,00	0,00	0,00	1,20	0,00	**1,20**
									[E.19] Fugas de información	1,37%		5%				0,00	0,35	0,00	0,00	0,00	**0,35**
									[E.20] Vulnerabilidades de los prog	1,37%		5%	5%	5%		0,00	0,35	0,25	0,30	0,00	**0,35**
									[E.24] Caída del sistema por agota	0,03%				80%		0,00	0,00	0,00	4,80	0,00	**4,80**
									[A.5] Suplantación de la identidad d	0,27%	80%	80%	50%			0,80	5,60	2,50	0,00	0,00	**5,60**
									[A.6] Abuso de privilegios de acces	1,37%		1%	1%	1%		0,00	0,07	0,05	0,06	0,00	**0,07**
									[A.7] Uso no previsto	13,70%		1%	1%	1%		0,00	0,07	0,05	0,06	0,00	**0,07**
									[A.9] [Re-]encaminamiento de mer	0,09%		80%				0,00	5,60	0,00	0,00	0,00	**5,60**
									[A.10] Alteración de secuencia	0,09%			50%			0,00	0,00	2,50	0,00	0,00	**2,50**
									[A.11] Acceso no autorizado	0,27%		50%	50%			0,00	3,50	2,50	0,00	0,00	**3,50**
									[A.13] Repudio	0,82%				10%		0,00	0,00	0,00	0,00	0,10	**0,10**
									[A.15] Modificación deliberada de l	0,09%			80%			0,00	0,00	4,00	0,00	0,00	**4,00**
									[A.18] Destrucción de información	0,09%				80%		0,00	0,00	0,00	4,80	0,00	**4,80**
									[A.19] Divulgación de información	0,09%		80%				0,00	5,60	0,00	0,00	0,00	**5,60**
									[A.24] Denegación de servicio	0,09%				80%		0,00	0,00	0,00	4,80	0,00	**4,80**
Activos Esenciales	[I] Información relativa a Oport	-	MA	1	7			4	[E.1] Errores de los usuarios	5,48%		10%	10%	10%		0,00	0,70	0,00	0,40	0,00	**0,70**
									[E.2] Errores del administrador	1,10%		20%	20%	20%		0,00	1,40	0,00	0,80	0,00	**1,40**
									[E.15] Alteración accidental de la ir	2,74%			5%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[E.18] Destrucción de información	2,74%				30%		0,00	0,00	0,00	1,20	0,00	**1,20**
									[E.19] Fugas de información	1,37%		10%				0,00	0,70	0,00	0,00	0,00	**0,70**
									[A.5] Suplantación de la identidad d	0,27%	80%	80%	50%			0,80	5,60	0,00	0,00	0,00	**5,60**
									[A.6] Abuso de privilegios de acces	2,74%		5%	5%	5%		0,00	0,35	0,00	0,20	0,00	**0,35**
									[A.11] Acceso no autorizado	0,27%		60%	60%			0,00	4,20	0,00	0,00	0,00	**4,20**
									[A.15] Modificación deliberada de l	0,09%			80%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.18] Destrucción de información	0,09%				80%		0,00	0,00	0,00	3,20	0,00	**3,20**
									[A.19] Divulgación de información	0,09%		80%				0,00	5,60	0,00	0,00	0,00	**5,60**
Activos Esenciales	[I] Información relativa a la Eje	-	MA	2	9			4	[E.1] Errores de los usuarios	5,48%		10%	10%	10%		0,00	0,90	0,00	0,40	0,00	**0,90**
									[E.2] Errores del administrador	1,10%		20%	20%	20%		0,00	1,80	0,00	0,80	0,00	**1,80**
									[E.15] Alteración accidental de la ir	2,74%			5%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[E.18] Destrucción de información	2,74%				30%		0,00	0,00	0,00	1,20	0,00	**1,20**
									[E.19] Fugas de información	1,37%		10%				0,00	0,90	0,00	0,00	0,00	**0,90**
									[A.5] Suplantación de la identidad d	0,27%	80%	80%	50%			1,60	7,20	0,00	0,00	0,00	**7,20**
									[A.6] Abuso de privilegios de acces	2,74%		5%	5%	5%		0,00	0,45	0,00	0,20	0,00	**0,45**
									[A.11] Acceso no autorizado	0,27%		60%	60%			0,00	5,40	0,00	0,00	0,00	**5,40**
									[A.15] Modificación deliberada de l	0,09%			80%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.18] Destrucción de información	0,09%				80%		0,00	0,00	0,00	3,20	0,00	**3,20**
									[A.19] Divulgación de información	0,09%		80%				0,00	7,20	0,00	0,00	0,00	**7,20**
Instalaciones	[L] CPD	Hardware	A					8	[N.1] Fuego	0,01%				20%		0,00	0,00	0,00	1,60	0,00	**1,60**
									[N.2] Daños por agua	0,00%				5%		0,00	0,00	0,00	0,40	0,00	**0,40**
									[N.*] Desastres naturales	0,00%				80%		0,00	0,00	0,00	6,40	0,00	**6,40**
									[I.1] Fuego	0,03%				20%		0,00	0,00	0,00	1,60	0,00	**1,60**
									[I.2] Daños por agua	0,27%				5%		0,00	0,00	0,00	0,40	0,00	**0,40**

									[I.*] Desastres industriales	0,27%				0%		0,00	0,00	0,00	0,01	0,00	**0,01**
									[I.11] Emanaciones electromagnéti	0,01%		80%				0,00	0,00	0,00	0,00	0,00	**0,00**
									[E.15] Alteración accidental de la ir	1,37%			1%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[E.18] Destrucción de información	1,37%				1%		0,00	0,00	0,00	0,08	0,00	**0,08**
									E.19] Fugas de información	1,37%		1%				0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.7] Uso no previsto	27,40%		0%	0%	0%		0,00	0,00	0,00	0,01	0,00	**0,01**
									[A.11] Acceso no autorizado	2,74%		1%	1%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.15] Modificación deliberada de l	0,03%			50%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.18] Destrucción de información	0,03%				1%		0,00	0,00	0,00	0,08	0,00	**0,08**
									[A.19] Divulgación de información	0,27%		50%				0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.26] Ataque destructivo	0,01%				20%		0,00	0,00	0,00	1,60	0,00	**1,60**
									[A.27] Ocupación enemiga	0,00%		50%		50%		0,00	0,00	0,00	4,00	0,00	**4,00**
Instalaciones	[L] Oficina	Hardware	MB				3		[N.1] Fuego	0,01%				20%		0,00	0,00	0,00	0,60	0,00	**0,60**
									[N.2] Daños por agua	0,00%				5%		0,00	0,00	0,00	0,15	0,00	**0,15**
									[N.*] Desastres naturales	0,00%				80%		0,00	0,00	0,00	2,40	0,00	**2,40**
									[I.1] Fuego	0,03%				20%		0,00	0,00	0,00	0,60	0,00	**0,60**
									[I.2] Daños por agua	0,27%				5%		0,00	0,00	0,00	0,15	0,00	**0,15**
									[I.*] Desastres industriales	0,27%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[I.11] Emanaciones electromagnéti	0,01%		80%				0,00	0,00	0,00	0,00	0,00	**0,00**
									[E.15] Alteración accidental de la ir	1,37%			1%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[E.18] Destrucción de información	1,37%				1%		0,00	0,00	0,00	0,03	0,00	**0,03**
									E.19] Fugas de información	1,37%		1%				0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.7] Uso no previsto	27,40%		0%	0%	0%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.11] Acceso no autorizado	2,74%		1%	1%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.15] Modificación deliberada de l	0,03%			50%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.18] Destrucción de información	0,03%				1%		0,00	0,00	0,00	0,03	0,00	**0,03**
									[A.19] Divulgación de información	0,27%		50%				0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.26] Ataque destructivo	0,01%				20%		0,00	0,00	0,00	0,60	0,00	**0,60**
									[A.27] Ocupación enemiga	0,00%		50%		50%		0,00	0,00	0,00	1,50	0,00	**1,50**
Hardware	[HW] Cabinas de discos	Aplicaciones	A	7	6	7	6	5	[N.1] Fuego	0,01%				20%		0,00	0,00	0,00	1,20	0,00	**1,20**
									[N.2] Daños por agua	0,00%				5%		0,00	0,00	0,00	0,30	0,00	**0,30**
									[N.*] Desastres naturales	0,00%				80%		0,00	0,00	0,00	4,80	0,00	**4,80**
									[I.1] Fuego	0,03%				50%		0,00	0,00	0,00	3,00	0,00	**3,00**
									[I.2] Daños por agua	0,27%				10%		0,00	0,00	0,00	0,60	0,00	**0,60**
									[I.*] Desastres industriales	0,27%				0%		0,00	0,00	0,00	0,01	0,00	**0,01**
									[I.3] Contaminación mecánica	0,27%				1%		0,00	0,00	0,00	0,06	0,00	**0,06**
									[I.4] Contaminación electromagnéti	2,74%				1%		0,00	0,00	0,00	0,06	0,00	**0,06**
									[I.5] Avería de origen físico o lógico	27,40%				5%		0,00	0,00	0,00	0,30	0,00	**0,30**
									[I.6] Corte del suministro eléctrico	0,27%				1%		0,00	0,00	0,00	0,06	0,00	**0,06**
									[I.7] Condiciones inadecuadas de t	0,27%				1%		0,00	0,00	0,00	0,06	0,00	**0,06**
									[I.11] Emanaciones electromagnéti	0,01%		80%				0,00	4,80	0,00	0,00	0,00	**4,80**
									[E.2] Errores del administrador	1,10%		20%	20%	20%		0,00	1,20	1,40	1,20	0,00	**1,40**
									[E.23] Errores de mantenimiento /	0,27%		20%	20%	20%		0,00	1,20	1,40	1,20	0,00	**1,40**
									[E.24] Caída del sistema por agota	0,09%				80%		0,00	0,00	0,00	4,80	0,00	**4,80**
									[E.25] Pérdida de equipos	1,37%		50%		10%		0,00	3,00	0,00	0,60	0,00	**3,00**
									[A.6] Abuso de privilegios de acces	2,74%		1%	1%	1%		0,00	0,06	0,07	0,06	0,00	**0,07**
									[A.7] Uso no previsto	27,40%		1%	1%	1%		0,00	0,06	0,07	0,06	0,00	**0,07**
									[A.11] Acceso no autorizado	0,09%		50%	50%			0,00	3,00	3,50	0,00	0,00	**3,50**
									[A.23] Manipulación de los equipos	0,09%		50%		80%		0,00	3,00	0,00	4,80	0,00	**4,80**

								[A.24] Denegación de servicio	0,09%			80%	0,00	0,00	0,00	4,80	0,00	**4,80**
								[A.25] Robo	1,37%	50%		10%	0,00	3,00	0,00	0,60	0,00	**3,00**
								[A.26] Ataque destructivo	0,03%			50%	0,00	0,00	0,00	3,00	0,00	**3,00**
Hardware	[HW] Dispositivos móviles (sm	Aplicaciones	B		6	3	1	[N.1] Fuego	0,01%			20%	0,00	0,00	0,00	0,20	0,00	**0,20**
								[N.2] Daños por agua	0,00%			5%	0,00	0,00	0,00	0,05	0,00	**0,05**
								[N.*] Desastres naturales	0,00%			80%	0,00	0,00	0,00	0,80	0,00	**0,80**
								[I.1] Fuego	0,03%			50%	0,00	0,00	0,00	0,50	0,00	**0,50**
								[I.2] Daños por agua	0,27%			10%	0,00	0,00	0,00	0,10	0,00	**0,10**
								[I.*] Desastres industriales	0,27%			0%	0,00	0,00	0,00	0,00	0,00	**0,00**
								[I.3] Contaminación mecánica	0,27%			1%	0,00	0,00	0,00	0,01	0,00	**0,01**
								[I.4] Contaminación electromagnéti	2,74%			1%	0,00	0,00	0,00	0,01	0,00	**0,01**
								[I.5] Avería de origen físico o lógico	27,40%			5%	0,00	0,00	0,00	0,05	0,00	**0,05**
								[I.6] Corte del suministro eléctrico	0,27%			1%	0,00	0,00	0,00	0,01	0,00	**0,01**
								[I.7] Condiciones inadecuadas de t	0,27%			1%	0,00	0,00	0,00	0,01	0,00	**0,01**
								[I.11] Emanaciones electromagnéti	0,01%	80%			0,00	4,80	0,00	0,00	0,00	**4,80**
								[E.2] Errores del administrador	1,10%	20%	20%	20%	0,00	1,20	0,60	0,20	0,00	**1,20**
								[E.23] Errores de mantenimiento /	0,27%	20%	20%	20%	0,00	1,20	0,60	0,20	0,00	**1,20**
								[E.24] Caída del sistema por agota	0,09%			80%	0,00	0,00	0,00	0,80	0,00	**0,80**
								[E.25] Pérdida de equipos	1,37%	50%		10%	0,00	3,00	0,00	0,10	0,00	**3,00**
								[A.6] Abuso de privilegios de acces	2,74%	1%	1%	1%	0,00	0,06	0,03	0,01	0,00	**0,06**
								[A.7] Uso no previsto	27,40%	1%	1%	1%	0,00	0,06	0,03	0,01	0,00	**0,06**
								[A.11] Acceso no autorizado	0,09%	50%	50%		0,00	3,00	1,50	0,00	0,00	**3,00**
								[A.23] Manipulación de los equipos	0,09%	50%		80%	0,00	3,00	0,00	0,80	0,00	**3,00**
								[A.24] Denegación de servicio	0,09%			80%	0,00	0,00	0,00	0,80	0,00	**0,80**
								[A.25] Robo	1,37%	50%		10%	0,00	3,00	0,00	0,10	0,00	**3,00**
								[A.26] Ataque destructivo	0,03%			50%	0,00	0,00	0,00	0,50	0,00	**0,50**
Hardware	[HW] Proxy de navegación	Aplicaciones	B				3	[N.1] Fuego	0,01%			20%	0,00	0,00	0,00	0,60	0,00	**0,60**
								[N.2] Daños por agua	0,00%			5%	0,00	0,00	0,00	0,15	0,00	**0,15**
								[N.*] Desastres naturales	0,00%			80%	0,00	0,00	0,00	2,40	0,00	**2,40**
								[I.1] Fuego	0,03%			50%	0,00	0,00	0,00	1,50	0,00	**1,50**
								[I.2] Daños por agua	0,27%			10%	0,00	0,00	0,00	0,30	0,00	**0,30**
								[I.*] Desastres industriales	0,27%			0%	0,00	0,00	0,00	0,00	0,00	**0,00**
								[I.3] Contaminación mecánica	0,27%			1%	0,00	0,00	0,00	0,03	0,00	**0,03**
								[I.4] Contaminación electromagnéti	2,74%			1%	0,00	0,00	0,00	0,03	0,00	**0,03**
								[I.5] Avería de origen físico o lógico	27,40%			5%	0,00	0,00	0,00	0,15	0,00	**0,15**
								[I.6] Corte del suministro eléctrico	0,27%			1%	0,00	0,00	0,00	0,03	0,00	**0,03**
								[I.7] Condiciones inadecuadas de t	0,27%			1%	0,00	0,00	0,00	0,03	0,00	**0,03**
								[I.11] Emanaciones electromagnéti	0,01%	80%			0,00	0,00	0,00	0,00	0,00	**0,00**
								[E.2] Errores del administrador	1,10%	20%	20%	20%	0,00	0,00	0,00	0,60	0,00	**0,60**
								[E.23] Errores de mantenimiento /	0,27%	20%	20%	20%	0,00	0,00	0,00	0,60	0,00	**0,60**
								[E.24] Caída del sistema por agota	0,09%			80%	0,00	0,00	0,00	2,40	0,00	**2,40**
								[E.25] Pérdida de equipos	1,37%	50%		10%	0,00	0,00	0,00	0,30	0,00	**0,30**
								[A.6] Abuso de privilegios de acces	2,74%	1%	1%	1%	0,00	0,00	0,00	0,03	0,00	**0,03**
								[A.7] Uso no previsto	27,40%	1%	1%	1%	0,00	0,00	0,00	0,03	0,00	**0,03**
								[A.11] Acceso no autorizado	0,09%	50%	50%		0,00	0,00	0,00	0,00	0,00	**0,00**
								[A.23] Manipulación de los equipos	0,09%	50%		80%	0,00	0,00	0,00	2,40	0,00	**2,40**
								[A.24] Denegación de servicio	0,09%			80%	0,00	0,00	0,00	2,40	0,00	**2,40**
								[A.25] Robo	1,37%	50%		10%	0,00	0,00	0,00	0,30	0,00	**0,30**
								[A.26] Ataque destructivo	0,03%			50%	0,00	0,00	0,00	1,50	0,00	**1,50**

Hardware	[HW] Puestos de trabajo (desk	Aplicaciones	M		7	5	2		[N.1] Fuego	0,01%				20%		0,00	0,00	0,00	0,40	0,00	**0,40**
									[N.2] Daños por agua	0,00%				5%		0,00	0,00	0,00	0,10	0,00	**0,10**
									[N.*] Desastres naturales	0,00%				80%		0,00	0,00	0,00	1,60	0,00	**1,60**
									[I.1] Fuego	0,03%				50%		0,00	0,00	0,00	1,00	0,00	**1,00**
									[I.2] Daños por agua	0,27%				10%		0,00	0,00	0,00	0,20	0,00	**0,20**
									[I.*] Desastres industriales	0,27%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[I.3] Contaminación mecánica	0,27%				1%		0,00	0,00	0,00	0,02	0,00	**0,02**
									[I.4] Contaminación electromagnéti	2,74%				1%		0,00	0,00	0,00	0,02	0,00	**0,02**
									[I.5] Avería de origen físico o lógico	27,40%				5%		0,00	0,00	0,00	0,10	0,00	**0,10**
									[I.6] Corte del suministro eléctrico	0,27%				1%		0,00	0,00	0,00	0,02	0,00	**0,02**
									[I.7] Condiciones inadecuadas de t	0,27%				1%		0,00	0,00	0,00	0,02	0,00	**0,02**
									[I.11] Emanaciones electromagnéti	0,01%		80%				0,00	5,60	0,00	0,00	0,00	**5,60**
									[E.2] Errores del administrador	1,10%		20%	20%	20%		0,00	1,40	1,00	0,40	0,00	**1,40**
									[E.23] Errores de mantenimiento /	0,27%		20%	20%	20%		0,00	1,40	1,00	0,40	0,00	**1,40**
									[E.24] Caída del sistema por agota	0,09%				80%		0,00	0,00	0,00	1,60	0,00	**1,60**
									[E.25] Pérdida de equipos	1,37%		50%		10%		0,00	3,50	0,00	0,20	0,00	**3,50**
									[A.6] Abuso de privilegios de acces	2,74%		1%	1%	1%		0,00	0,07	0,05	0,02	0,00	**0,07**
									[A.7] Uso no previsto	27,40%		1%	1%	1%		0,00	0,07	0,05	0,02	0,00	**0,07**
									[A.11] Acceso no autorizado	0,09%		50%	50%			0,00	3,50	2,50	0,00	0,00	**3,50**
									[A.23] Manipulación de los equipos	0,09%		50%		80%		0,00	3,50	0,00	1,60	0,00	**3,50**
									[A.24] Denegación de servicio	0,09%				80%		0,00	0,00	0,00	1,60	0,00	**1,60**
									[A.25] Robo	1,37%		50%		10%		0,00	3,50	0,00	0,20	0,00	**3,50**
									[A.26] Ataque destructivo	0,03%				50%		0,00	0,00	0,00	1,00	0,00	**1,00**
Hardware	[HW] Servidores en CPD	Aplicaciones	A	7	6	6	6	5	[N.1] Fuego	0,01%				20%		0,00	0,00	0,00	1,20	0,00	**1,20**
									[N.2] Daños por agua	0,00%				5%		0,00	0,00	0,00	0,30	0,00	**0,30**
									[N.*] Desastres naturales	0,00%				80%		0,00	0,00	0,00	4,80	0,00	**4,80**
									[I.1] Fuego	0,03%				50%		0,00	0,00	0,00	3,00	0,00	**3,00**
									[I.2] Daños por agua	0,27%				10%		0,00	0,00	0,00	0,60	0,00	**0,60**
									[I.*] Desastres industriales	0,27%				0%		0,00	0,00	0,00	0,01	0,00	**0,01**
									[I.3] Contaminación mecánica	0,27%				1%		0,00	0,00	0,00	0,06	0,00	**0,06**
									[I.4] Contaminación electromagnéti	2,74%				1%		0,00	0,00	0,00	0,06	0,00	**0,06**
									[I.5] Avería de origen físico o lógico	27,40%				5%		0,00	0,00	0,00	0,30	0,00	**0,30**
									[I.6] Corte del suministro eléctrico	0,27%				1%		0,00	0,00	0,00	0,06	0,00	**0,06**
									[I.7] Condiciones inadecuadas de t	0,27%				1%		0,00	0,00	0,00	0,06	0,00	**0,06**
									[I.11] Emanaciones electromagnéti	0,01%		80%				0,00	4,80	0,00	0,00	0,00	**4,80**
									[E.2] Errores del administrador	1,10%		20%	20%	20%		0,00	1,20	1,20	1,20	0,00	**1,20**
									[E.23] Errores de mantenimiento /	0,27%		20%	20%	20%		0,00	1,20	1,20	1,20	0,00	**1,20**
									[E.24] Caída del sistema por agota	0,09%				80%		0,00	0,00	0,00	4,80	0,00	**4,80**
									[E.25] Pérdida de equipos	1,37%		50%		10%		0,00	3,00	0,00	0,60	0,00	**3,00**
									[A.6] Abuso de privilegios de acces	2,74%		1%	1%	1%		0,00	0,06	0,06	0,06	0,00	**0,06**
									[A.7] Uso no previsto	27,40%		1%	1%	1%		0,00	0,06	0,06	0,06	0,00	**0,06**
									[A.11] Acceso no autorizado	0,09%		50%	50%			0,00	3,00	3,00	0,00	0,00	**3,00**
									[A.23] Manipulación de los equipos	0,09%		50%		80%		0,00	3,00	0,00	4,80	0,00	**4,80**
									[A.24] Denegación de servicio	0,09%				80%		0,00	0,00	0,00	4,80	0,00	**4,80**
									[A.25] Robo	1,37%		50%		10%		0,00	3,00	0,00	0,60	0,00	**3,00**
									[A.26] Ataque destructivo	0,03%				50%		0,00	0,00	0,00	3,00	0,00	**3,00**
Hardware	[HW] Sistemas de impresión	Aplicaciones	MB				1		[N.1] Fuego	0,01%				20%		0,00	0,00	0,00	0,20	0,00	**0,20**
									[N.2] Daños por agua	0,00%				5%		0,00	0,00	0,00	0,05	0,00	**0,05**
									[N.*] Desastres naturales	0,00%				80%		0,00	0,00	0,00	0,80	0,00	**0,80**

									[I.1] Fuego	0,03%				50%		0,00	0,00	0,00	0,50	0,00	**0,50**
									[I.2] Daños por agua	0,27%				10%		0,00	0,00	0,00	0,10	0,00	**0,10**
									[I.*] Desastres industriales	0,27%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[I.3] Contaminación mecánica	0,27%				1%		0,00	0,00	0,00	0,01	0,00	**0,01**
									[I.4] Contaminación electromagnéti	2,74%				1%		0,00	0,00	0,00	0,01	0,00	**0,01**
									[I.5] Avería de origen físico o lógico	27,40%				5%		0,00	0,00	0,00	0,05	0,00	**0,05**
									[I.6] Corte del suministro eléctrico	0,27%				1%		0,00	0,00	0,00	0,01	0,00	**0,01**
									[I.7] Condiciones inadecuadas de t	0,27%				1%		0,00	0,00	0,00	0,01	0,00	**0,01**
									[I.11] Emanaciones electromagnéti	0,01%		80%				0,00	0,00	0,00	0,00	0,00	**0,00**
									[E.2] Errores del administrador	1,10%		20%	20%	20%		0,00	0,00	0,00	0,20	0,00	**0,20**
									[E.23] Errores de mantenimiento /	0,27%		20%	20%	20%		0,00	0,00	0,00	0,20	0,00	**0,20**
									[E.24] Caída del sistema por agota	0,09%				80%		0,00	0,00	0,00	0,80	0,00	**0,80**
									[E.25] Pérdida de equipos	1,37%		50%		10%		0,00	0,00	0,00	0,10	0,00	**0,10**
									[A.6] Abuso de privilegios de acces	2,74%		1%	1%	1%		0,00	0,00	0,00	0,01	0,00	**0,01**
									[A.7] Uso no previsto	27,40%		1%	1%	1%		0,00	0,00	0,00	0,01	0,00	**0,01**
									[A.11] Acceso no autorizado	0,09%		50%	50%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.23] Manipulación de los equipos	0,09%		50%		80%		0,00	0,00	0,00	0,80	0,00	**0,80**
									[A.24] Denegación de servicio	0,09%				80%		0,00	0,00	0,00	0,80	0,00	**0,80**
									[A.25] Robo	1,37%		50%		10%		0,00	0,00	0,00	0,10	0,00	**0,10**
									[A.26] Ataque destructivo	0,03%				50%		0,00	0,00	0,00	0,50	0,00	**0,50**
Aplicaciones	[SW] Antivirus/antimalware	Datos	M				4		[I.5] Avería de origen físico o lógico	0,55%				5%		0,00	0,00	0,00	0,20	0,00	**0,20**
									[E.1] Errores de los usuarios	5,48%		5%	5%	5%		0,00	0,00	0,00	0,20	0,00	**0,20**
									[E.2] Errores del administrador	1,10%		20%	20%	20%		0,00	0,00	0,00	0,80	0,00	**0,80**
									[E.8] Difusión de software dañino	0,27%		80%	80%	80%		0,00	0,00	0,00	3,20	0,00	**3,20**
									[E.9] Errores de [re-]encaminamien	0,27%		10%				0,00	0,00	0,00	0,00	0,00	**0,00**
									[E.10] Errores de secuencia	1,37%			5%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[E.15] Alteración accidental de la ir	2,74%			5%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[E.18] Destrucción de información	2,74%				20%		0,00	0,00	0,00	0,80	0,00	**0,80**
									[E.19] Fugas de información	1,37%		5%				0,00	0,00	0,00	0,00	0,00	**0,00**
									[E.20] Vulnerabilidades de los prog	1,37%		5%	5%	5%		0,00	0,00	0,00	0,20	0,00	**0,20**
									[E.21] Errores de mantenimiento /	2,74%		1%	1%	1%		0,00	0,00	0,00	0,04	0,00	**0,04**
									[A.5] Suplantación de la identidad	0,27%	80%	80%	50%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.6] Abuso de privilegios de acces	2,74%		1%	1%	1%		0,00	0,00	0,00	0,04	0,00	**0,04**
									[A.7] Uso no previsto	27,40%		1%	1%	1%		0,00	0,00	0,00	0,04	0,00	**0,04**
									[A.8] Difusión de software dañino	0,27%		50%	50%	80%		0,00	0,00	0,00	3,20	0,00	**3,20**
									[A.9] [Re-]encaminamiento de men	0,09%		80%				0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.10] Alteración de secuencia	0,09%			50%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.11] Acceso no autorizado	0,27%		50%	50%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.15] Modificación deliberada de l	0,09%			80%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.18] Destrucción de información	0,09%				80%		0,00	0,00	0,00	3,20	0,00	**3,20**
									[A.19] Divulgación de información	0,09%		80%				0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.22] Manipulación de programas	0,03%		80%	80%	80%		0,00	0,00	0,00	3,20	0,00	**3,20**
Aplicaciones	[SW] Aplicaciones a medida de	Datos	M		5	5	3		[I.5] Avería de origen físico o lógico	0,55%				5%		0,00	0,00	0,00	0,15	0,00	**0,15**
									[E.1] Errores de los usuarios	5,48%		5%	5%	5%		0,00	0,25	0,25	0,15	0,00	**0,25**
									[E.2] Errores del administrador	1,10%		20%	20%	20%		0,00	1,00	1,00	0,60	0,00	**1,00**
									[E.8] Difusión de software dañino	0,27%		80%	80%	80%		0,00	4,00	4,00	2,40	0,00	**4,00**
									[E.9] Errores de [re-]encaminamien	0,27%		10%				0,00	0,50	0,00	0,00	0,00	**0,50**
									[E.10] Errores de secuencia	1,37%			5%			0,00	0,00	0,25	0,00	0,00	**0,25**
									[E.15] Alteración accidental de la ir	2,74%			5%			0,00	0,00	0,25	0,00	0,00	**0,25**

								[E.18] Destrucción de información	2,74%				20%		0,00	0,00	0,00	0,60	0,00	**0,60**
								[E.19] Fugas de información	1,37%		5%				0,00	0,25	0,00	0,00	0,00	**0,25**
								[E.20] Vulnerabilidades de los prog	1,37%		5%	5%	5%		0,00	0,25	0,25	0,15	0,00	**0,25**
								[E.21] Errores de mantenimiento /	2,74%		1%	1%	1%		0,00	0,05	0,05	0,03	0,00	**0,05**
								[A.5] Suplantación de la identidad d	0,27%	80%	80%	50%			0,00	4,00	2,50	0,00	0,00	**4,00**
								[A.6] Abuso de privilegios de acces	2,74%		1%	1%	1%		0,00	0,05	0,05	0,03	0,00	**0,05**
								[A.7] Uso no previsto	27,40%		1%	1%	1%		0,00	0,05	0,05	0,03	0,00	**0,05**
								[A.8] Difusión de software dañino	0,27%		50%	50%	80%		0,00	2,50	2,50	2,40	0,00	**2,50**
								[A.9] [Re-]encaminamiento de mer	0,09%		80%				0,00	4,00	0,00	0,00	0,00	**4,00**
								[A.10] Alteración de secuencia	0,09%			50%			0,00	0,00	2,50	0,00	0,00	**2,50**
								[A.11] Acceso no autorizado	0,27%		50%	50%			0,00	2,50	2,50	0,00	0,00	**2,50**
								[A.15] Modificación deliberada de l	0,09%			80%			0,00	0,00	4,00	0,00	0,00	**4,00**
								[A.18] Destrucción de información	0,09%				80%		0,00	0,00	0,00	2,40	0,00	**2,40**
								[A.19] Divulgación de información	0,09%		80%				0,00	4,00	0,00	0,00	0,00	**4,00**
								[A.22] Manipulación de programas	0,03%		80%	80%	80%		0,00	4,00	4,00	2,40	0,00	**4,00**
Aplicaciones	[SW] Aplicaciones ofimáticas	Datos	B				4	[I.5] Avería de origen físico o lógico	0,55%				5%		0,00	0,00	0,00	0,20	0,00	**0,20**
								[E.1] Errores de los usuarios	5,48%		5%	5%	5%		0,00	0,00	0,00	0,20	0,00	**0,20**
								[E.2] Errores del administrador	1,10%		20%	20%	20%		0,00	0,00	0,00	0,80	0,00	**0,80**
								[E.8] Difusión de software dañino	0,27%		80%	80%	80%		0,00	0,00	0,00	3,20	0,00	**3,20**
								[E.9] Errores de [re-]encaminamier	0,27%		10%				0,00	0,00	0,00	0,00	0,00	**0,00**
								[E.10] Errores de secuencia	1,37%			5%			0,00	0,00	0,00	0,00	0,00	**0,00**
								[E.15] Alteración accidental de la ir	2,74%			5%			0,00	0,00	0,00	0,00	0,00	**0,00**
								[E.18] Destrucción de información	2,74%				20%		0,00	0,00	0,00	0,80	0,00	**0,80**
								[E.19] Fugas de información	1,37%		5%				0,00	0,00	0,00	0,00	0,00	**0,00**
								[E.20] Vulnerabilidades de los prog	1,37%		5%	5%	5%		0,00	0,00	0,00	0,20	0,00	**0,20**
								[E.21] Errores de mantenimiento /	2,74%		1%	1%	1%		0,00	0,00	0,00	0,04	0,00	**0,04**
								[A.5] Suplantación de la identidad d	0,27%	80%	80%	50%			0,00	0,00	0,00	0,00	0,00	**0,00**
								[A.6] Abuso de privilegios de acces	2,74%		1%	1%	1%		0,00	0,00	0,00	0,04	0,00	**0,04**
								[A.7] Uso no previsto	27,40%		1%	1%	1%		0,00	0,00	0,00	0,04	0,00	**0,04**
								[A.8] Difusión de software dañino	0,27%		50%	50%	80%		0,00	0,00	0,00	3,20	0,00	**3,20**
								[A.9] [Re-]encaminamiento de mer	0,09%		80%				0,00	0,00	0,00	0,00	0,00	**0,00**
								[A.10] Alteración de secuencia	0,09%			50%			0,00	0,00	0,00	0,00	0,00	**0,00**
								[A.11] Acceso no autorizado	0,27%		50%	50%			0,00	0,00	0,00	0,00	0,00	**0,00**
								[A.15] Modificación deliberada de l	0,09%			80%			0,00	0,00	0,00	0,00	0,00	**0,00**
								[A.18] Destrucción de información	0,09%				80%		0,00	0,00	0,00	3,20	0,00	**3,20**
								[A.19] Divulgación de información	0,09%		80%				0,00	0,00	0,00	0,00	0,00	**0,00**
								[A.22] Manipulación de programas	0,03%		80%	80%	80%		0,00	0,00	0,00	3,20	0,00	**3,20**
Aplicaciones	[SW] Aplicación de backup	Datos	M		6	8	5	[I.5] Avería de origen físico o lógico	0,55%				5%		0,00	0,00	0,00	0,25	0,00	**0,25**
								[E.1] Errores de los usuarios	5,48%		5%	5%	5%		0,00	0,30	0,40	0,25	0,00	**0,40**
								[E.2] Errores del administrador	1,10%		20%	20%	20%		0,00	1,20	1,60	1,00	0,00	**1,60**
								[E.8] Difusión de software dañino	0,27%		80%	80%	80%		0,00	4,80	6,40	4,00	0,00	**6,40**
								[E.9] Errores de [re-]encaminamier	0,27%		10%				0,00	0,60	0,00	0,00	0,00	**0,60**
								[E.10] Errores de secuencia	1,37%			5%			0,00	0,00	0,40	0,00	0,00	**0,40**
								[E.15] Alteración accidental de la ir	2,74%			5%			0,00	0,00	0,40	0,00	0,00	**0,40**
								[E.18] Destrucción de información	2,74%				20%		0,00	0,00	0,00	1,00	0,00	**1,00**
								[E.19] Fugas de información	1,37%		5%				0,00	0,30	0,00	0,00	0,00	**0,30**
								[E.20] Vulnerabilidades de los prog	1,37%		5%	5%	5%		0,00	0,30	0,40	0,25	0,00	**0,40**
								[E.21] Errores de mantenimiento /	2,74%		1%	1%	1%		0,00	0,06	0,08	0,05	0,00	**0,08**
								[A.5] Suplantación de la identidad d	0,27%	80%	80%	50%			0,00	4,80	4,00	0,00	0,00	**4,80**

									[A.6] Abuso de privilegios de acces	2,74%		1%	1%	1%		0,00	0,06	0,08	0,05	0,00	**0,08**
									[A.7] Uso no previsto	27,40%		1%	1%	1%		0,00	0,06	0,08	0,05	0,00	**0,08**
									[A.8] Difusión de software dañino	0,27%		50%	50%	80%		0,00	3,00	4,00	4,00	0,00	**4,00**
									[A.9] [Re-]encaminamiento de men	0,09%		80%				0,00	4,80	0,00	0,00	0,00	**4,80**
									[A.10] Alteración de secuencia	0,09%			50%			0,00	0,00	4,00	0,00	0,00	**4,00**
									[A.11] Acceso no autorizado	0,27%		50%	50%			0,00	3,00	4,00	0,00	0,00	**4,00**
									[A.15] Modificación deliberada de l	0,09%			80%			0,00	0,00	6,40	0,00	0,00	**6,40**
									[A.18] Destrucción de información	0,09%				80%		0,00	0,00	0,00	4,00	0,00	**4,00**
									[A.19] Divulgación de información	0,09%		80%				0,00	4,80	0,00	0,00	0,00	**4,80**
									[A.22] Manipulación de programas	0,03%		80%	80%	80%		0,00	4,80	6,40	4,00	0,00	**6,40**
Aplicaciones	[SW] Desarrollos propios	Datos	A		7	5	5		[I.5] Avería de origen físico o lógico	0,55%				5%		0,00	0,00	0,00	0,25	0,00	**0,25**
									[E.1] Errores de los usuarios	5,48%		5%	5%	5%		0,00	0,35	0,25	0,25	0,00	**0,35**
									[E.2] Errores del administrador	1,10%		20%	20%	20%		0,00	1,40	1,00	1,00	0,00	**1,40**
									[E.8] Difusión de software dañino	0,27%		80%	80%	80%		0,00	5,60	4,00	4,00	0,00	**5,60**
									[E.9] Errores de [re-]encaminamien	0,27%		10%				0,00	0,70	0,00	0,00	0,00	**0,70**
									[E.10] Errores de secuencia	1,37%			5%			0,00	0,00	0,25	0,00	0,00	**0,25**
									[E.15] Alteración accidental de la ir	2,74%			5%			0,00	0,00	0,25	0,00	0,00	**0,25**
									[E.18] Destrucción de información	2,74%				20%		0,00	0,00	0,00	1,00	0,00	**1,00**
									[E.19] Fugas de información	1,37%		5%				0,00	0,35	0,00	0,00	0,00	**0,35**
									[E.20] Vulnerabilidades de los prog	1,37%		5%	5%	5%		0,00	0,35	0,25	0,25	0,00	**0,35**
									[E.21] Errores de mantenimiento /	2,74%		1%	1%	1%		0,00	0,07	0,05	0,05	0,00	**0,07**
									[A.5] Suplantación de la identidad d	0,27%	80%	80%	50%			0,00	5,60	2,50	0,00	0,00	**5,60**
									[A.6] Abuso de privilegios de acces	2,74%		1%	1%	1%		0,00	0,07	0,05	0,05	0,00	**0,07**
									[A.7] Uso no previsto	27,40%		1%	1%	1%		0,00	0,07	0,05	0,05	0,00	**0,07**
									[A.8] Difusión de software dañino	0,27%		50%	50%	80%		0,00	3,50	2,50	4,00	0,00	**4,00**
									[A.9] [Re-]encaminamiento de men	0,09%		80%				0,00	5,60	0,00	0,00	0,00	**5,60**
									[A.10] Alteración de secuencia	0,09%			50%			0,00	0,00	2,50	0,00	0,00	**2,50**
									[A.11] Acceso no autorizado	0,27%		50%	50%			0,00	3,50	2,50	0,00	0,00	**3,50**
									[A.15] Modificación deliberada de l	0,09%			80%			0,00	0,00	4,00	0,00	0,00	**4,00**
									[A.18] Destrucción de información	0,09%				80%		0,00	0,00	0,00	4,00	0,00	**4,00**
									[A.19] Divulgación de información	0,09%		80%				0,00	5,60	0,00	0,00	0,00	**5,60**
									[A.22] Manipulación de programas	0,03%		80%	80%	80%		0,00	5,60	4,00	4,00	0,00	**5,60**
Datos	[D] Código fuente	**Activos Esenciales**	A	6	7	4	3	5	[E.1] Errores de los usuarios	5,48%		10%	10%	10%		0,00	0,70	0,40	0,30	0,00	**0,70**
									[E.2] Errores del administrador	1,10%		20%	20%	20%		0,00	1,40	0,80	0,60	0,00	**1,40**
									[E.15] Alteración accidental de la ir	2,74%			5%			0,00	0,00	0,20	0,00	0,00	**0,20**
									[E.18] Destrucción de información	2,74%				30%		0,00	0,00	0,00	0,90	0,00	**0,90**
									[E.19] Fugas de información	1,37%		10%				0,00	0,70	0,00	0,00	0,00	**0,70**
									[A.5] Suplantación de la identidad d	0,27%	80%	80%	50%			4,80	5,60	2,00	0,00	0,00	**5,60**
									[A.6] Abuso de privilegios de acces	2,74%		5%	5%	5%		0,00	0,35	0,20	0,15	0,00	**0,35**
									[A.11] Acceso no autorizado	0,27%		60%	60%			0,00	4,20	2,40	0,00	0,00	**4,20**
									[A.15] Modificación deliberada de l	0,09%			80%			0,00	0,00	3,20	0,00	0,00	**3,20**
									[A.18] Destrucción de información	0,09%				80%		0,00	0,00	0,00	2,40	0,00	**2,40**
									[A.19] Divulgación de información	0,09%		80%				0,00	5,60	0,00	0,00	0,00	**5,60**
Datos	[D] Documentos ofimáticos	**Activos Esenciales**	A	7	7	4	3	4	[E.1] Errores de los usuarios	5,48%		10%	10%	10%		0,00	0,70	0,40	0,30	0,00	**0,70**
									[E.2] Errores del administrador	1,10%		20%	20%	20%		0,00	1,40	0,80	0,60	0,00	**1,40**
									[E.15] Alteración accidental de la ir	2,74%			5%			0,00	0,00	0,20	0,00	0,00	**0,20**
									[E.18] Destrucción de información	2,74%				30%		0,00	0,00	0,00	0,90	0,00	**0,90**
									[E.19] Fugas de información	1,37%		10%				0,00	0,70	0,00	0,00	0,00	**0,70**
									[A.5] Suplantación de la identidad d	0,27%	80%	80%	50%			5,60	5,60	2,00	0,00	0,00	**5,60**

									[A.6] Abuso de privilegios de acces	2,74%		5%	5%	5%		0,00	0,35	0,20	0,15	0,00	**0,35**
									[A.11] Acceso no autorizado	0,27%		60%	60%			0,00	4,20	2,40	0,00	0,00	**4,20**
									[A.15] Modificación deliberada de l	0,09%			80%			0,00	0,00	3,20	0,00	0,00	**3,20**
									[A.18] Destrucción de información	0,09%				80%		0,00	0,00	0,00	2,40	0,00	**2,40**
									[A.19] Divulgación de información	0,09%		80%				0,00	5,60	0,00	0,00	0,00	**5,60**
Redes de Comunicaciones	[COM] Acceso a Internet	Datos	M		7	2	4		[I.8] Fallo de servicios de comunica	0,27%		80%				0,00	5,60	0,00	0,00	0,00	**5,60**
									[E.2] Errores del administrador	1,10%		10%	5%	50%		0,00	0,70	0,10	2,00	0,00	**2,00**
									[E.9] Errores de [re-]encaminamier	0,27%		10%				0,00	0,70	0,00	0,00	0,00	**0,70**
									[E.10] Errores de secuencia	0,05%			0%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[E.15] Alteración accidental de la ir	0,05%			0%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[E.18] Destrucción de información	0,05%				30%		0,00	0,00	0,00	1,20	0,00	**1,20**
									[E.19] Fugas de información	0,03%		0%				0,00	0,01	0,00	0,00	0,00	**0,01**
									[E.24] Caída del sistema por agota	0,09%				80%		0,00	0,00	0,00	3,20	0,00	**3,20**
									[A.5] Suplantación de la identidad d	0,27%	80%	80%	50%			0,00	5,60	1,00	0,00	0,00	**5,60**
									[A.6] Abuso de privilegios de acces	2,74%		1%	1%	1%		0,00	0,07	0,02	0,04	0,00	**0,07**
									[A.7] Uso no previsto	27,40%		1%	1%	1%		0,00	0,07	0,02	0,04	0,00	**0,07**
									[A.9] [Re-]encaminamiento de men	0,09%		80%				0,00	5,60	0,00	0,00	0,00	**5,60**
									[A.10] Alteración de secuencia	0,09%			50%			0,00	0,00	1,00	0,00	0,00	**1,00**
									[A.11] Acceso no autorizado	0,27%		50%	50%			0,00	3,50	1,00	0,00	0,00	**3,50**
									[A.12] Análisis de tráfico	0,09%		50%				0,00	3,50	0,00	0,00	0,00	**3,50**
									[A.14] Interceptación de informació	0,05%		80%				0,00	5,60	0,00	0,00	0,00	**5,60**
									[A.15] Modificación deliberada de l	0,09%			80%			0,00	0,00	1,60	0,00	0,00	**1,60**
									[A.19] Divulgación de información	0,09%		80%				0,00	5,60	0,00	0,00	0,00	**5,60**
									[A.24] Denegación de servicio	0,09%				80%		0,00	0,00	0,00	3,20	0,00	**3,20**
Redes de Comunicaciones	[COM] Comunicaciones LAN/W	Datos	B		5	5	4		[I.8] Fallo de servicios de comunica	0,27%		80%				0,00	4,00	0,00	0,00	0,00	**4,00**
									[E.2] Errores del administrador	1,10%		10%	5%	50%		0,00	0,50	0,25	2,00	0,00	**2,00**
									[E.9] Errores de [re-]encaminamier	0,27%		10%				0,00	0,50	0,00	0,00	0,00	**0,50**
									[E.10] Errores de secuencia	0,05%			0%			0,00	0,00	0,01	0,00	0,00	**0,01**
									[E.15] Alteración accidental de la ir	0,05%			0%			0,00	0,00	0,01	0,00	0,00	**0,01**
									[E.18] Destrucción de información	0,05%				30%		0,00	0,00	0,00	1,20	0,00	**1,20**
									[E.19] Fugas de información	0,03%		0%				0,00	0,01	0,00	0,00	0,00	**0,01**
									[E.24] Caída del sistema por agota	0,09%				80%		0,00	0,00	0,00	3,20	0,00	**3,20**
									[A.5] Suplantación de la identidad d	0,27%	80%	80%	50%			0,00	4,00	2,50	0,00	0,00	**4,00**
									[A.6] Abuso de privilegios de acces	2,74%		1%	1%	1%		0,00	0,05	0,05	0,04	0,00	**0,05**
									[A.7] Uso no previsto	27,40%		1%	1%	1%		0,00	0,05	0,05	0,04	0,00	**0,05**
									[A.9] [Re-]encaminamiento de men	0,09%		80%				0,00	4,00	0,00	0,00	0,00	**4,00**
									[A.10] Alteración de secuencia	0,09%			50%			0,00	0,00	2,50	0,00	0,00	**2,50**
									[A.11] Acceso no autorizado	0,27%		50%	50%			0,00	2,50	2,50	0,00	0,00	**2,50**
									[A.12] Análisis de tráfico	0,09%		50%				0,00	2,50	0,00	0,00	0,00	**2,50**
									[A.14] Interceptación de informació	0,05%		80%				0,00	4,00	0,00	0,00	0,00	**4,00**
									[A.15] Modificación deliberada de l	0,09%			80%			0,00	0,00	4,00	0,00	0,00	**4,00**
									[A.19] Divulgación de información	0,09%		80%				0,00	4,00	0,00	0,00	0,00	**4,00**
									[A.24] Denegación de servicio	0,09%				80%		0,00	0,00	0,00	3,20	0,00	**3,20**
Servicios Auxiliares	[SS] Servicios en formato Saa§	Datos	M		6	6	7		[E.1] Errores de los usuarios	5,48%		5%	5%	5%		0,00	0,30	0,30	0,35	0,00	**0,35**
									[E.2] Errores del administrador	1,10%		20%	20%	20%		0,00	1,20	1,20	1,40	0,00	**1,40**
									[E.9] Errores de [re-]encaminamier	0,27%		10%				0,00	0,60	0,00	0,00	0,00	**0,60**
									[E.10] Errores de secuencia	1,37%			5%			0,00	0,00	0,30	0,00	0,00	**0,30**
									[E.15] Alteración accidental de la ir	2,74%			5%			0,00	0,00	0,30	0,00	0,00	**0,30**
									[E.18] Destrucción de información	2,74%				20%		0,00	0,00	0,00	1,40	0,00	**1,40**
									[E.19] Fugas de información	1,37%		5%				0,00	0,30	0,00	0,00	0,00	**0,30**

									[E.20] Vulnerabilidades de los prog	1,37%		5%	5%	5%		0,00	0,30	0,30	0,35	0,00	**0,35**
									[E.24] Caída del sistema por agota	0,03%				80%		0,00	0,00	0,00	5,60	0,00	**5,60**
									[A.5] Suplantación de la identidad (	0,27%	80%	80%	50%			0,00	4,80	3,00	0,00	0,00	**4,80**
									[A.6] Abuso de privilegios de acces	1,37%		1%	1%	1%		0,00	0,06	0,06	0,07	0,00	**0,07**
									[A.7] Uso no previsto	13,70%		1%	1%	1%		0,00	0,06	0,06	0,07	0,00	**0,07**
									[A.9] [Re-]encaminamiento de men	0,09%		80%				0,00	4,80	0,00	0,00	0,00	**4,80**
									[A.10] Alteración de secuencia	0,09%			50%			0,00	0,00	3,00	0,00	0,00	**3,00**
									[A.11] Acceso no autorizado	0,27%		50%	50%			0,00	3,00	3,00	0,00	0,00	**3,00**
									[A.13] Repudio	0,82%					10%	0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.15] Modificación deliberada de l	0,09%			80%			0,00	0,00	4,80	0,00	0,00	**4,80**
									[A.18] Destrucción de información	0,09%				80%		0,00	0,00	0,00	5,60	0,00	**5,60**
									[A.19] Divulgación de información	0,09%		80%				0,00	4,80	0,00	0,00	0,00	**4,80**
									[A.24] Denegación de servicio	0,09%				80%		0,00	0,00	0,00	5,60	0,00	**5,60**
Servicios Auxiliares	[SS] Servidores en formato laa	Datos	B	7	6	6	6	5	[E.1] Errores de los usuarios	5,48%		5%	5%	5%		0,00	0,30	0,30	0,30	0,00	**0,30**
									[E.2] Errores del administrador	1,10%		20%	20%	20%		0,00	1,20	1,20	1,20	0,00	**1,20**
									[E.9] Errores de [re-]encaminamier	0,27%		10%				0,00	0,60	0,00	0,00	0,00	**0,60**
									[E.10] Errores de secuencia	1,37%			5%			0,00	0,00	0,30	0,00	0,00	**0,30**
									[E.15] Alteración accidental de la ir	2,74%			5%			0,00	0,00	0,30	0,00	0,00	**0,30**
									[E.18] Destrucción de información	2,74%				20%		0,00	0,00	0,00	1,20	0,00	**1,20**
									[E.19] Fugas de información	1,37%		5%				0,00	0,30	0,00	0,00	0,00	**0,30**
									[E.20] Vulnerabilidades de los prog	1,37%		5%	5%	5%		0,00	0,30	0,30	0,30	0,00	**0,30**
									[E.24] Caída del sistema por agota	0,03%				80%		0,00	0,00	0,00	4,80	0,00	**4,80**
									[A.5] Suplantación de la identidad (	0,27%	80%	80%	50%			5,60	4,80	3,00	0,00	0,00	**5,60**
									[A.6] Abuso de privilegios de acces	1,37%		1%	1%	1%		0,00	0,06	0,06	0,06	0,00	**0,06**
									[A.7] Uso no previsto	13,70%		1%	1%	1%		0,00	0,06	0,06	0,06	0,00	**0,06**
									[A.9] [Re-]encaminamiento de men	0,09%		80%				0,00	4,80	0,00	0,00	0,00	**4,80**
									[A.10] Alteración de secuencia	0,09%			50%			0,00	0,00	3,00	0,00	0,00	**3,00**
									[A.11] Acceso no autorizado	0,27%		50%	50%			0,00	3,00	3,00	0,00	0,00	**3,00**
									[A.13] Repudio	0,82%					10%	0,00	0,00	0,00	0,00	0,50	**0,50**
									[A.15] Modificación deliberada de l	0,09%			80%			0,00	0,00	4,80	0,00	0,00	**4,80**
									[A.18] Destrucción de información	0,09%				80%		0,00	0,00	0,00	4,80	0,00	**4,80**
									[A.19] Divulgación de información	0,09%		80%				0,00	4,80	0,00	0,00	0,00	**4,80**
									[A.24] Denegación de servicio	0,09%				80%		0,00	0,00	0,00	4,80	0,00	**4,80**
Equipamiento Auxiliar	[Media] CD-Rom, DVD, Memo	Datos	MB		8	2			[N.1] Fuego	0,01%				2%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[N.2] Daños por agua	0,00%				1%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[N.*] Desastres naturales	0,00%				8%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[I.1] Fuego	0,03%				5%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[I.2] Daños por agua	0,27%				1%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[I.*] Desastres industriales	0,27%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[I.3] Contaminación mecánica	0,27%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[I.4] Contaminación electromagnéti	2,74%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[I.5] Avería de origen físico o lógico	27,40%				1%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[I.6] Corte del suministro eléctrico	0,27%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[I.7] Condiciones inadecuadas de t	0,27%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[I.9] Interrupción de otros servicios	0,27%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[I.10] Degradación de los soportes	0,05%				20%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[I.11] Emanaciones electromagnéti	0,00%		16%				0,00	1,28	0,00	0,00	0,00	**1,28**
									[E.1] Errores de los usuarios	5,48%		1%	1%	1%		0,00	0,08	0,02	0,00	0,00	**0,08**
									[E.2] Errores del administrador	1,10%		4%	4%	4%		0,00	0,32	0,08	0,00	0,00	**0,32**

								[E.15] Alteración accidental de la ir	2,74%			1%			0,00	0,00	0,02	0,00	0,00	**0,02**
								[E.18] Destrucción de información	2,74%				2%		0,00	0,00	0,00	0,00	0,00	**0,00**
								[E.19] Fugas de información	1,37%		5%				0,00	0,40	0,00	0,00	0,00	**0,40**
								[E.23] Errores de mantenimiento /	0,00%		4%	4%	2%		0,00	0,32	0,08	0,00	0,00	**0,32**
								[E.25] Pérdida de equipos	1,37%		10%		1%		0,00	0,80	0,00	0,00	0,00	**0,80**
								[A.7] Uso no previsto	27,40%		0%	0%	0%		0,00	0,02	0,00	0,00	0,00	**0,02**
								[A.11] Acceso no autorizado	0,09%		10%	10%			0,00	0,80	0,20	0,00	0,00	**0,80**
								[A.15] Modificación deliberada de l	0,09%			16%			0,00	0,00	0,32	0,00	0,00	**0,32**
								[A.18] Destrucción de información	0,09%				8%		0,00	0,00	0,00	0,00	0,00	**0,00**
								[A.19] Divulgación de información	0,09%		16%				0,00	1,28	0,00	0,00	0,00	**1,28**
								[A.23] Manipulación de los equipos	0,09%		10%		8%		0,00	0,80	0,00	0,00	0,00	**0,80**
								[A.25] Robo	1,37%		10%		1%		0,00	0,80	0,00	0,00	0,00	**0,80**
								[A.26] Ataque destructivo	0,03%				5%		0,00	0,00	0,00	0,00	0,00	**0,00**
Equipamiento Auxiliar	[Media] Documentación en for	Datos	MB		4		2	[N.1] Fuego	0,01%				2%		0,00	0,00	0,00	0,04	0,00	**0,04**
								[N.2] Daños por agua	0,00%				1%		0,00	0,00	0,00	0,01	0,00	**0,01**
								[N.*] Desastres naturales	0,00%				8%		0,00	0,00	0,00	0,16	0,00	**0,16**
								[I.1] Fuego	0,03%				5%		0,00	0,00	0,00	0,10	0,00	**0,10**
								[I.2] Daños por agua	0,27%				1%		0,00	0,00	0,00	0,02	0,00	**0,02**
								[I.*] Desastres industriales	0,27%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
								[I.3] Contaminación mecánica	0,27%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
								[I.4] Contaminación electromagnéti	2,74%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
								[I.5] Avería de origen físico o lógico	27,40%				1%		0,00	0,00	0,00	0,01	0,00	**0,01**
								[I.6] Corte del suministro eléctrico	0,27%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
								[I.7] Condiciones inadecuadas de t	0,27%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
								[I.9] Interrupción de otros servicios	0,27%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
								[I.10] Degradación de los soportes	0,05%				20%		0,00	0,00	0,00	0,40	0,00	**0,40**
								[I.11] Emanaciones electromagnéti	0,00%		16%				0,00	0,64	0,00	0,00	0,00	**0,64**
								[E.1] Errores de los usuarios	5,48%		1%	1%	1%		0,00	0,04	0,00	0,02	0,00	**0,04**
								[E.2] Errores del administrador	1,10%		4%	4%	4%		0,00	0,16	0,00	0,08	0,00	**0,16**
								[E.15] Alteración accidental de la ir	2,74%			1%			0,00	0,00	0,00	0,00	0,00	**0,00**
								[E.18] Destrucción de información	2,74%				2%		0,00	0,00	0,00	0,04	0,00	**0,04**
								[E.19] Fugas de información	1,37%		5%				0,00	0,20	0,00	0,00	0,00	**0,20**
								[E.23] Errores de mantenimiento /	0,00%		4%	4%	2%		0,00	0,16	0,00	0,04	0,00	**0,16**
								[E.25] Pérdida de equipos	1,37%		10%		1%		0,00	0,40	0,00	0,02	0,00	**0,40**
								[A.7] Uso no previsto	27,40%		0%	0%	0%		0,00	0,01	0,00	0,00	0,00	**0,01**
								[A.11] Acceso no autorizado	0,09%		10%	10%			0,00	0,40	0,00	0,00	0,00	**0,40**
								[A.15] Modificación deliberada de l	0,09%			16%			0,00	0,00	0,00	0,00	0,00	**0,00**
								[A.18] Destrucción de información	0,09%				8%		0,00	0,00	0,00	0,16	0,00	**0,16**
								[A.19] Divulgación de información	0,09%		16%				0,00	0,64	0,00	0,00	0,00	**0,64**
								[A.23] Manipulación de los equipos	0,09%		10%		8%		0,00	0,40	0,00	0,16	0,00	**0,40**
								[A.25] Robo	1,37%		10%		1%		0,00	0,40	0,00	0,02	0,00	**0,40**
								[A.26] Ataque destructivo	0,03%				5%		0,00	0,00	0,00	0,10	0,00	**0,10**
Equipamiento Auxiliar	[AUX] Destructora de documer	Datos	MB				2	[N.1] Fuego	0,01%				2%		0,00	0,00	0,00	0,04	0,00	**0,04**
								[N.2] Daños por agua	0,00%				1%		0,00	0,00	0,00	0,01	0,00	**0,01**
								[N.*] Desastres naturales	0,00%				8%		0,00	0,00	0,00	0,16	0,00	**0,16**
								[I.1] Fuego	0,03%				5%		0,00	0,00	0,00	0,10	0,00	**0,10**
								[I.2] Daños por agua	0,27%				1%		0,00	0,00	0,00	0,02	0,00	**0,02**
								[I.*] Desastres industriales	0,27%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
								[I.3] Contaminación mecánica	0,27%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**

					[I.4] Contaminación electromagnéti	2,74%			0%	0,00	0,00	0,00	0,00	0,00	**0,00**
					[I.5] Avería de origen físico o lógico	27,40%			1%	0,00	0,00	0,00	0,01	0,00	**0,01**
					[I.6] Corte del suministro eléctrico	0,27%			0%	0,00	0,00	0,00	0,00	0,00	**0,00**
					[I.7] Condiciones inadecuadas de t	0,27%			0%	0,00	0,00	0,00	0,00	0,00	**0,00**
					[I.9] Interrupción de otros servicios	0,27%			0%	0,00	0,00	0,00	0,00	0,00	**0,00**
					[I.10] Degradación de los soportes	0,05%			20%	0,00	0,00	0,00	0,40	0,00	**0,40**
					[I.11] Emanaciones electromagnéti	0,00%	16%			0,00	0,00	0,00	0,00	0,00	**0,00**
					[E.1] Errores de los usuarios	5,48%	1%	1%	1%	0,00	0,00	0,00	0,02	0,00	**0,02**
					[E.2] Errores del administrador	1,10%	4%	4%	4%	0,00	0,00	0,00	0,08	0,00	**0,08**
					[E.15] Alteración accidental de la ir	2,74%		1%		0,00	0,00	0,00	0,00	0,00	**0,00**
					[E.18] Destrucción de información	2,74%			2%	0,00	0,00	0,00	0,04	0,00	**0,04**
					[E.19] Fugas de información	1,37%	5%			0,00	0,00	0,00	0,00	0,00	**0,00**
					[E.23] Errores de mantenimiento /	0,00%	4%	4%	2%	0,00	0,00	0,00	0,04	0,00	**0,04**
					[E.25] Pérdida de equipos	1,37%	10%		1%	0,00	0,00	0,00	0,02	0,00	**0,02**
					[A.7] Uso no previsto	27,40%	0%	0%	0%	0,00	0,00	0,00	0,00	0,00	**0,00**
					[A.11] Acceso no autorizado	0,09%	10%	10%		0,00	0,00	0,00	0,00	0,00	**0,00**
					[A.15] Modificación deliberada de l	0,09%		16%		0,00	0,00	0,00	0,00	0,00	**0,00**
					[A.18] Destrucción de información	0,09%			8%	0,00	0,00	0,00	0,16	0,00	**0,16**
					[A.19] Divulgación de información	0,09%	16%			0,00	0,00	0,00	0,00	0,00	**0,00**
					[A.23] Manipulación de los equipos	0,09%	10%		8%	0,00	0,00	0,00	0,16	0,00	**0,16**
					[A.25] Robo	1,37%	10%		1%	0,00	0,00	0,00	0,02	0,00	**0,02**
					[A.26] Ataque destructivo	0,03%			5%	0,00	0,00	0,00	0,10	0,00	**0,10**
Equipamiento Auxiliar	[AUX] Sistema de cableado	Datos	MB	1	[N.1] Fuego	0,01%			2%	0,00	0,00	0,00	0,02	0,00	**0,02**
					[N.2] Daños por agua	0,00%			1%	0,00	0,00	0,00	0,01	0,00	**0,01**
					[N.*] Desastres naturales	0,00%			8%	0,00	0,00	0,00	0,08	0,00	**0,08**
					[I.1] Fuego	0,03%			5%	0,00	0,00	0,00	0,05	0,00	**0,05**
					[I.2] Daños por agua	0,27%			1%	0,00	0,00	0,00	0,01	0,00	**0,01**
					[I.*] Desastres industriales	0,27%			0%	0,00	0,00	0,00	0,00	0,00	**0,00**
					[I.3] Contaminación mecánica	0,27%			0%	0,00	0,00	0,00	0,00	0,00	**0,00**
					[I.4] Contaminación electromagnéti	2,74%			0%	0,00	0,00	0,00	0,00	0,00	**0,00**
					[I.5] Avería de origen físico o lógico	27,40%			1%	0,00	0,00	0,00	0,01	0,00	**0,01**
					[I.6] Corte del suministro eléctrico	0,27%			0%	0,00	0,00	0,00	0,00	0,00	**0,00**
					[I.7] Condiciones inadecuadas de t	0,27%			0%	0,00	0,00	0,00	0,00	0,00	**0,00**
					[I.9] Interrupción de otros servicios	0,27%			0%	0,00	0,00	0,00	0,00	0,00	**0,00**
					[I.10] Degradación de los soportes	0,05%			20%	0,00	0,00	0,00	0,20	0,00	**0,20**
					[I.11] Emanaciones electromagnéti	0,00%	16%			0,00	0,00	0,00	0,00	0,00	**0,00**
					[E.1] Errores de los usuarios	5,48%	1%	1%	1%	0,00	0,00	0,00	0,01	0,00	**0,01**
					[E.2] Errores del administrador	1,10%	4%	4%	4%	0,00	0,00	0,00	0,04	0,00	**0,04**
					[E.15] Alteración accidental de la ir	2,74%		1%		0,00	0,00	0,00	0,00	0,00	**0,00**
					[E.18] Destrucción de información	2,74%			2%	0,00	0,00	0,00	0,02	0,00	**0,02**
					[E.19] Fugas de información	1,37%	5%			0,00	0,00	0,00	0,00	0,00	**0,00**
					[E.23] Errores de mantenimiento /	0,00%	4%	4%	2%	0,00	0,00	0,00	0,02	0,00	**0,02**
					[E.25] Pérdida de equipos	1,37%	10%		1%	0,00	0,00	0,00	0,01	0,00	**0,01**
					[A.7] Uso no previsto	27,40%	0%	0%	0%	0,00	0,00	0,00	0,00	0,00	**0,00**
					[A.11] Acceso no autorizado	0,09%	10%	10%		0,00	0,00	0,00	0,00	0,00	**0,00**
					[A.15] Modificación deliberada de l	0,09%		16%		0,00	0,00	0,00	0,00	0,00	**0,00**
					[A.18] Destrucción de información	0,09%			8%	0,00	0,00	0,00	0,08	0,00	**0,08**
					[A.19] Divulgación de información	0,09%	16%			0,00	0,00	0,00	0,00	0,00	**0,00**
					[A.23] Manipulación de los equipos	0,09%	10%		8%	0,00	0,00	0,00	0,08	0,00	**0,08**
					[A.25] Robo	1,37%	10%		1%	0,00	0,00	0,00	0,01	0,00	**0,01**

									[A.26] Ataque destructivo	0,03%				5%		0,00	0,00	0,00	0,05	0,00	**0,05**
Equipamiento Auxiliar	[AUX] UPS, Generadores eléc	Datos	MB				4		[N.1] Fuego	0,01%				2%		0,00	0,00	0,00	0,08	0,00	**0,08**
									[N.2] Daños por agua	0,00%				1%		0,00	0,00	0,00	0,02	0,00	**0,02**
									[N.*] Desastres naturales	0,00%				8%		0,00	0,00	0,00	0,32	0,00	**0,32**
									[I.1] Fuego	0,03%				5%		0,00	0,00	0,00	0,20	0,00	**0,20**
									[I.2] Daños por agua	0,27%				1%		0,00	0,00	0,00	0,04	0,00	**0,04**
									[I.*] Desastres industriales	0,27%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[I.3] Contaminación mecánica	0,27%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[I.4] Contaminación electromagnéti	2,74%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[I.5] Avería de origen físico o lógico	27,40%				1%		0,00	0,00	0,00	0,02	0,00	**0,02**
									[I.6] Corte del suministro eléctrico	0,27%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[I.7] Condiciones inadecuadas de t	0,27%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[I.9] Interrupción de otros servicios	0,27%				0%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[I.10] Degradación de los soportes	0,05%				20%		0,00	0,00	0,00	0,80	0,00	**0,80**
									[I.11] Emanaciones electromagnéti	0,00%		16%				0,00	0,00	0,00	0,00	0,00	**0,00**
									[E.1] Errores de los usuarios	5,48%		1%	1%	1%		0,00	0,00	0,00	0,04	0,00	**0,04**
									[E.2] Errores del administrador	1,10%		4%	4%	4%		0,00	0,00	0,00	0,16	0,00	**0,16**
									[E.15] Alteración accidental de la in	2,74%			1%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[E.18] Destrucción de información	2,74%				2%		0,00	0,00	0,00	0,08	0,00	**0,08**
									[E.19] Fugas de información	1,37%		5%				0,00	0,00	0,00	0,00	0,00	**0,00**
									[E.23] Errores de mantenimiento /	0,00%		4%	4%	2%		0,00	0,00	0,00	0,08	0,00	**0,08**
									[E.25] Pérdida de equipos	1,37%		10%		1%		0,00	0,00	0,00	0,04	0,00	**0,04**
									[A.7] Uso no previsto	27,40%		0%	0%	0%		0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.11] Acceso no autorizado	0,09%		10%	10%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.15] Modificación deliberada de l	0,09%			16%			0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.18] Destrucción de información	0,09%				8%		0,00	0,00	0,00	0,32	0,00	**0,32**
									[A.19] Divulgación de información	0,09%		16%				0,00	0,00	0,00	0,00	0,00	**0,00**
									[A.23] Manipulación de los equipos	0,09%		10%		8%		0,00	0,00	0,00	0,32	0,00	**0,32**
									[A.25] Robo	1,37%		10%		1%		0,00	0,00	0,00	0,04	0,00	**0,04**
									[A.26] Ataque destructivo	0,03%				5%		0,00	0,00	0,00	0,20	0,00	**0,20**
Personal	[P] Administrador de comunica	**Activos Esenciales**	B				2		[E.7] Deficiencias en la organizació	1,10%				30%		0,00	0,00	0,00	0,60	0,00	**0,60**
									[E.19] Fugas de información	2,74%		10%				0,00	0,00	0,00	0,00	0,00	**0,00**
									[E.28] Indisponibilidad del personal	2,74%				30%		0,00	0,00	0,00	0,60	0,00	**0,60**
									[A.28] Indisponibilidad del personal	0,55%				30%		0,00	0,00	0,00	0,60	0,00	**0,60**
									[A.29] Extorsión	0,05%		50%	50%	50%		0,00	0,00	0,00	1,00	0,00	**1,00**
									[A.30] Ingeniería social (picaresca)	0,27%		30%	30%	30%		0,00	0,00	0,00	0,60	0,00	**0,60**
Personal	[P] Administrador de segurida	**Activos Esenciales**	B				3		[E.7] Deficiencias en la organizació	1,10%				30%		0,00	0,00	0,00	0,90	0,00	**0,90**
									[E.19] Fugas de información	2,74%		10%				0,00	0,00	0,00	0,00	0,00	**0,00**
									[E.28] Indisponibilidad del personal	2,74%				30%		0,00	0,00	0,00	0,90	0,00	**0,90**
									[A.28] Indisponibilidad del personal	0,55%				30%		0,00	0,00	0,00	0,90	0,00	**0,90**
									[A.29] Extorsión	0,05%		50%	50%	50%		0,00	0,00	0,00	1,50	0,00	**1,50**
									[A.30] Ingeniería social (picaresca)	0,27%		30%	30%	30%		0,00	0,00	0,00	0,90	0,00	**0,90**
Personal	[P] Administrador de sistemas	**Activos Esenciales**	B				2		[E.7] Deficiencias en la organizació	1,10%				30%		0,00	0,00	0,00	0,60	0,00	**0,60**
									[E.19] Fugas de información	2,74%		10%				0,00	0,00	0,00	0,00	0,00	**0,00**
									[E.28] Indisponibilidad del personal	2,74%				30%		0,00	0,00	0,00	0,60	0,00	**0,60**
									[A.28] Indisponibilidad del personal	0,55%				30%		0,00	0,00	0,00	0,60	0,00	**0,60**
									[A.29] Extorsión	0,05%		50%	50%	50%		0,00	0,00	0,00	1,00	0,00	**1,00**
									[A.30] Ingeniería social (picaresca)	0,27%		30%	30%	30%		0,00	0,00	0,00	0,60	0,00	**0,60**
Personal	[P] Usuarios	**Activos Esenciales**	B				2		[E.7] Deficiencias en la organizació	1,10%				30%		0,00	0,00	0,00	0,60	0,00	**0,60**

[E.19] Fugas de información	2,74%		10%				0,00	0,00	0,00	0,00	0,00	0,00	**0,00**
[E.28] Indisponibilidad del persona	2,74%				30%		0,00	0,00	0,00	0,60	0,00	0,00	**0,60**
[A.28] Indisponibilidad del persona	0,55%				30%		0,00	0,00	0,00	0,60	0,00	0,00	**0,60**
[A.29] Extorsión	0,05%			50%	50%		0,00	0,00	0,00	1,00	0,00	1,00	**1,00**
[A.30] Ingeniería social (picaresca)	0,27%			30%	30%		0,00	0,00	0,00	0,60	0,00	0,00	**0,60**

Tabla 17: Detalle de Impactos

6.3 Representaciones de Riesgos por Categoría de Activos

6.3.1 Activos Esenciales

- [S] Servicios de Ejecución de Proyectos
- [I] Información relativa a Oportunidades de Negocio / Operaciones de Preventa
- [I] Información relativa a la Ejecución de Proyecto

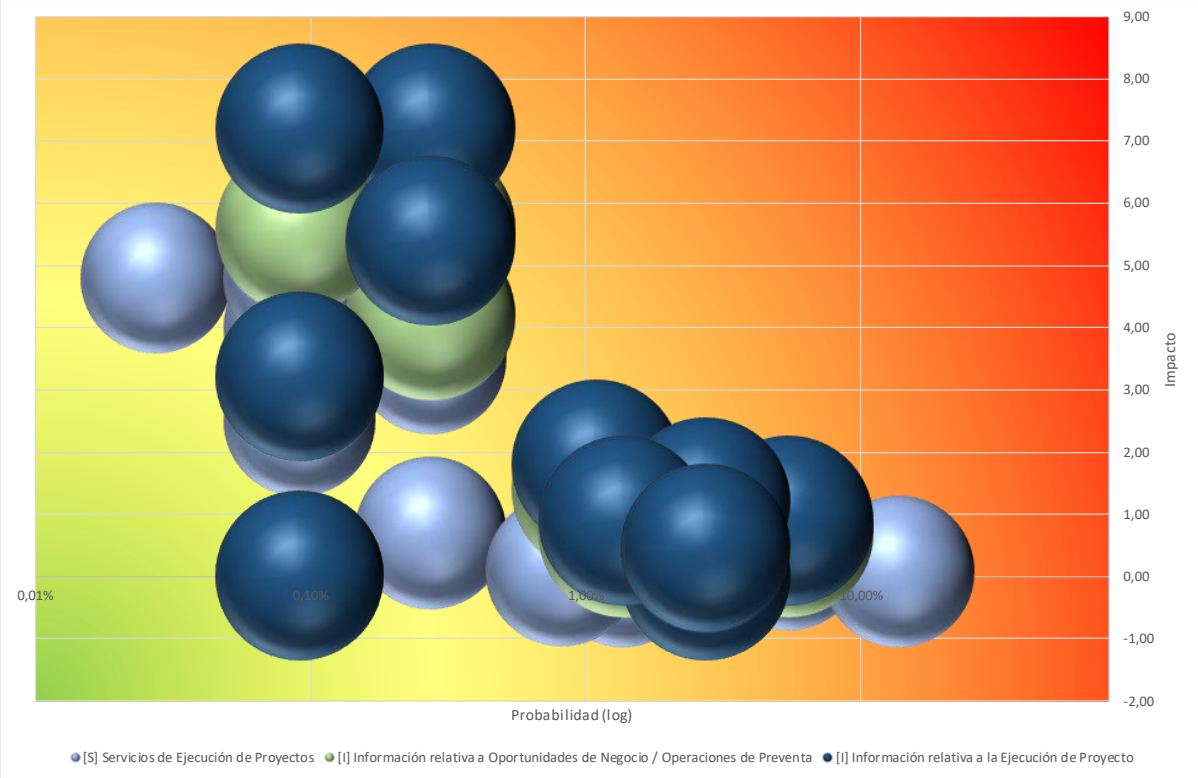


Imagen 29: Riesgos en Activos Esenciales

6.3.2 Instalaciones

- [L] CPD
- [L] Oficina

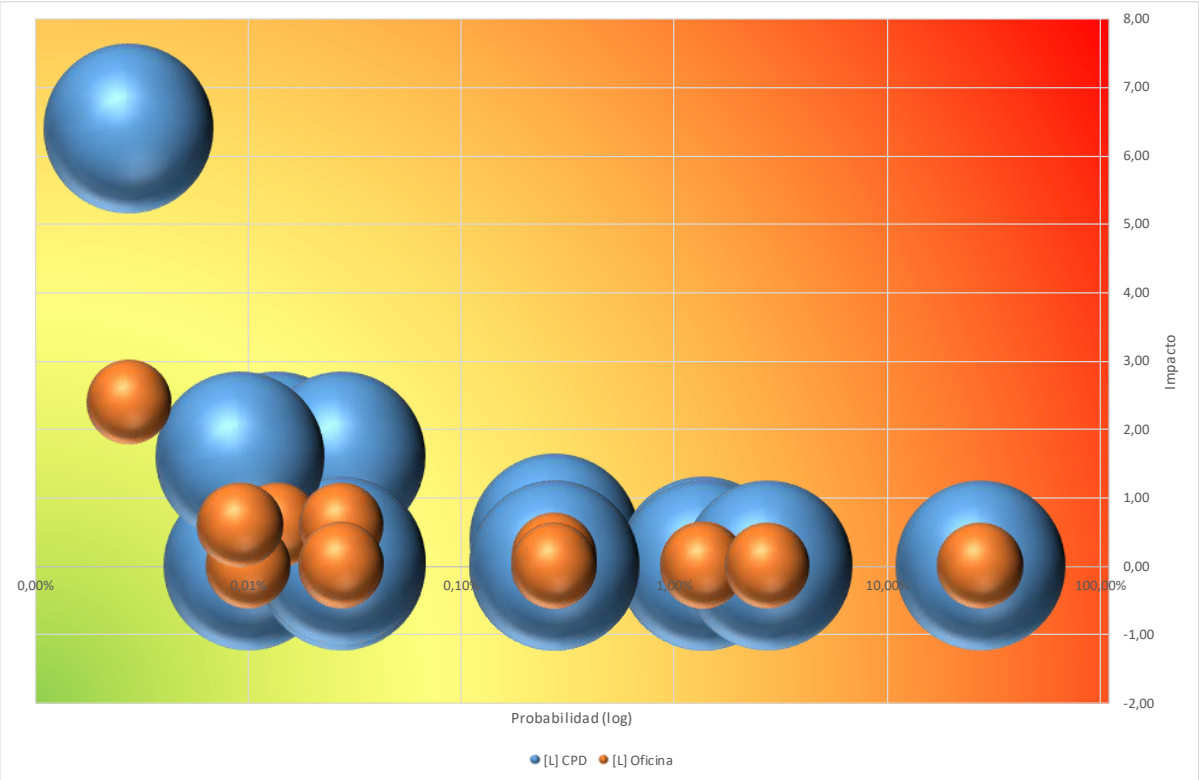


Imagen 30: Riesgos en Instalaciones

6.3.3 Hardware

- [HW] Cabinas de discos
- [HW] Dispositivos móviles (smartphones o tablets)
- [HW] Proxy de navegación
- [HW] Puestos de trabajo (desktops o laptops)
- [HW] Servidores en CPD
- [HW] Sistemas de impresión

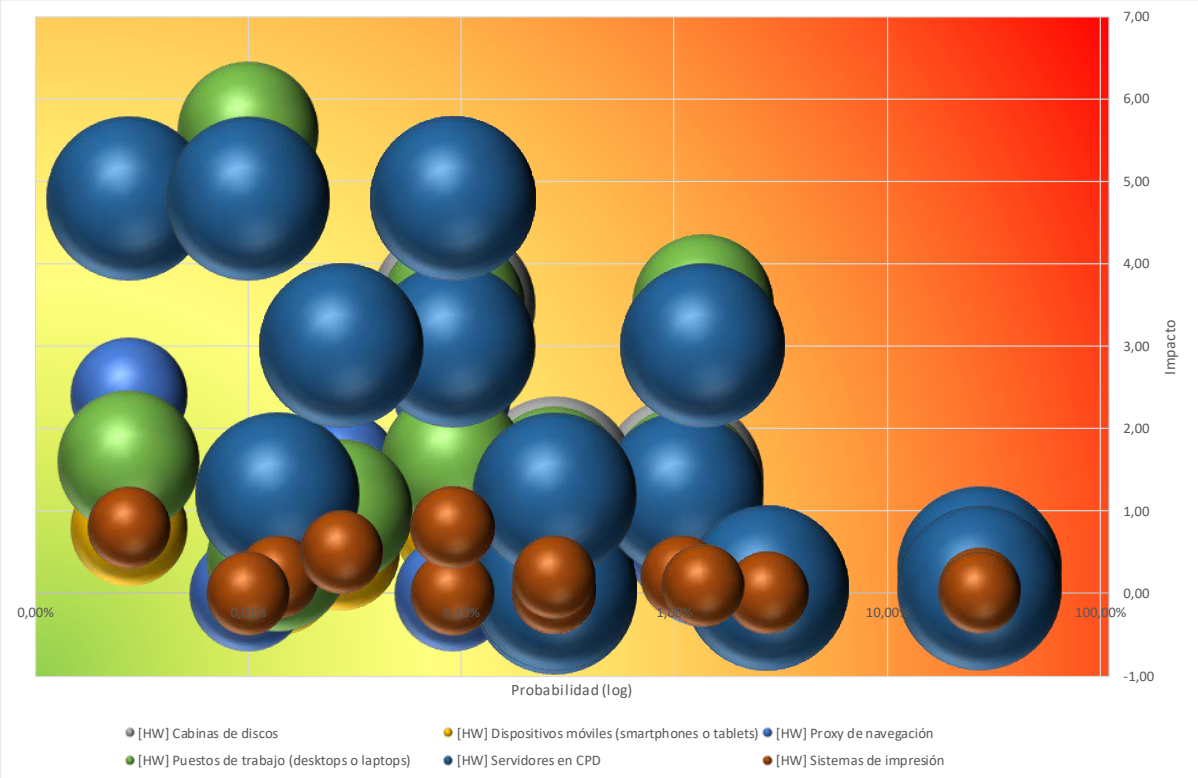


Imagen 31: Riesgos en Hardware

6.3.4 Aplicaciones

- [SW] Antivirus/antimalware
- [SW] Aplicaciones a medida de Gestión de Proyectos
- [SW] Aplicaciones ofimáticas
- [SW] Aplicación de backup
- [SW] Desarrollos propios

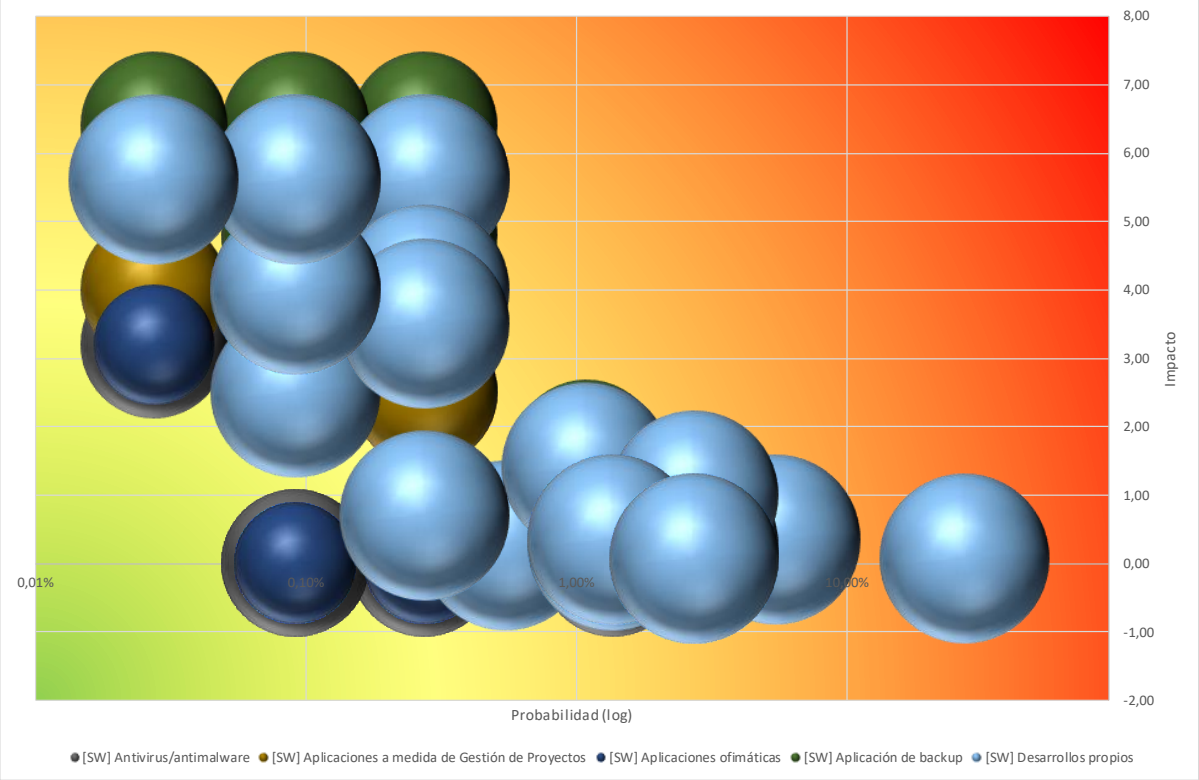


Imagen 32: Riesgos en Aplicaciones

6.3.5 Datos

- [D] Código fuente
- [D] Documentos ofimáticos

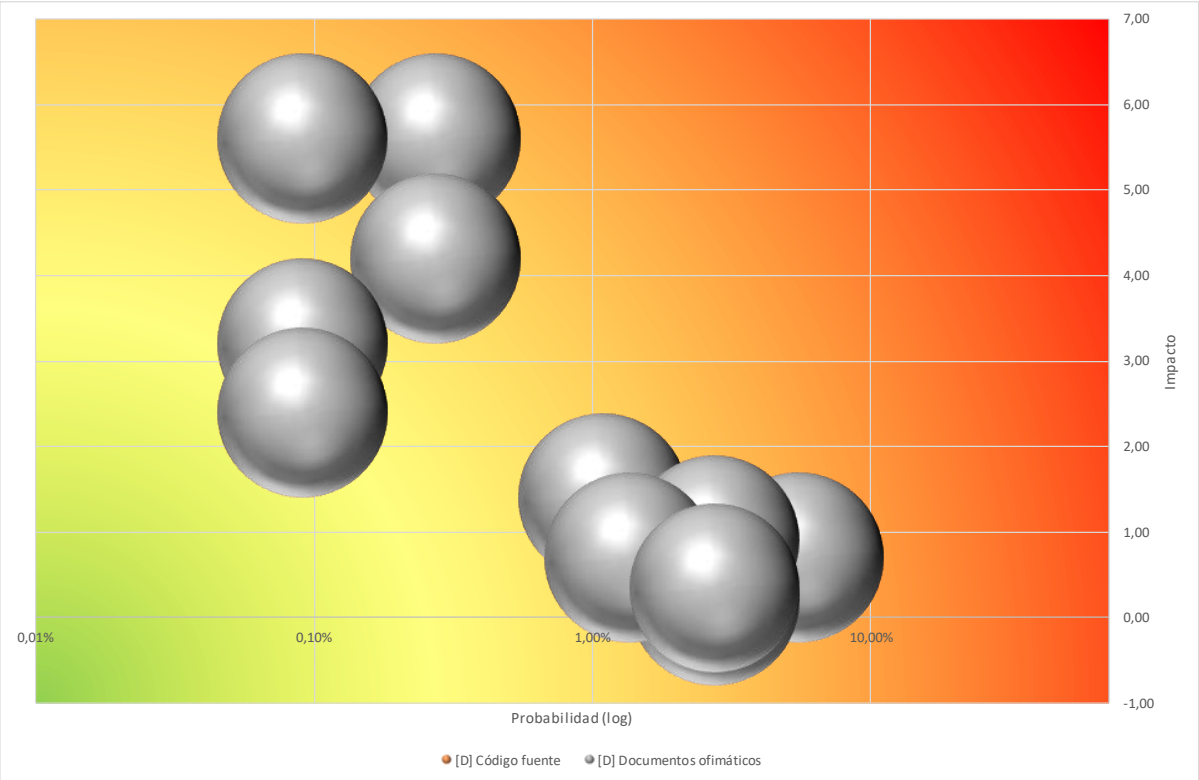


Imagen 33: Riesgos en Datos

6.3.6 Redes de Comunicaciones

- [COM] Acceso a Internet
- [COM] Comunicaciones LAN/WAN (electrónica de red, routers, firewalls, etc.)

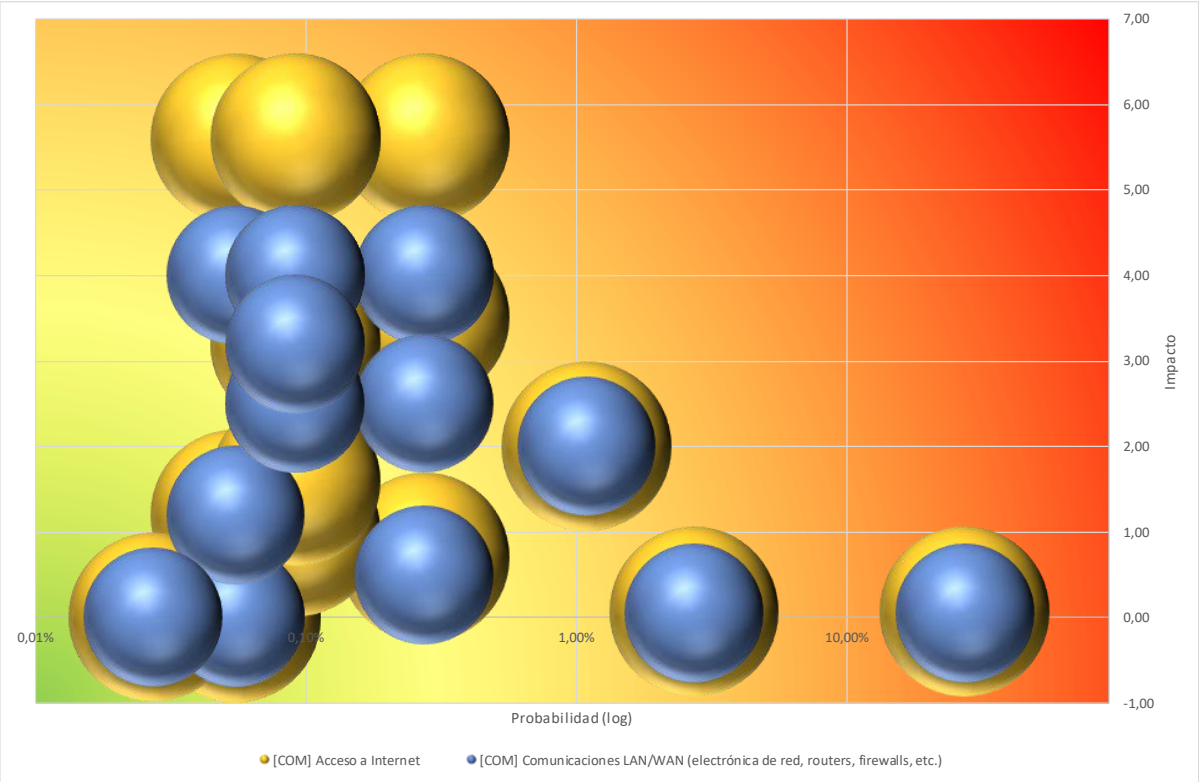


Imagen 34: Riesgos en Redes de Comunicaciones

6.3.7 Servicios Auxiliares

- [SS] Servicios en formato SaaS (Software as a Service): correo, MI, directorio, storage
- [SS] Servidores en formato IaaS (Infrastructure as a Service)

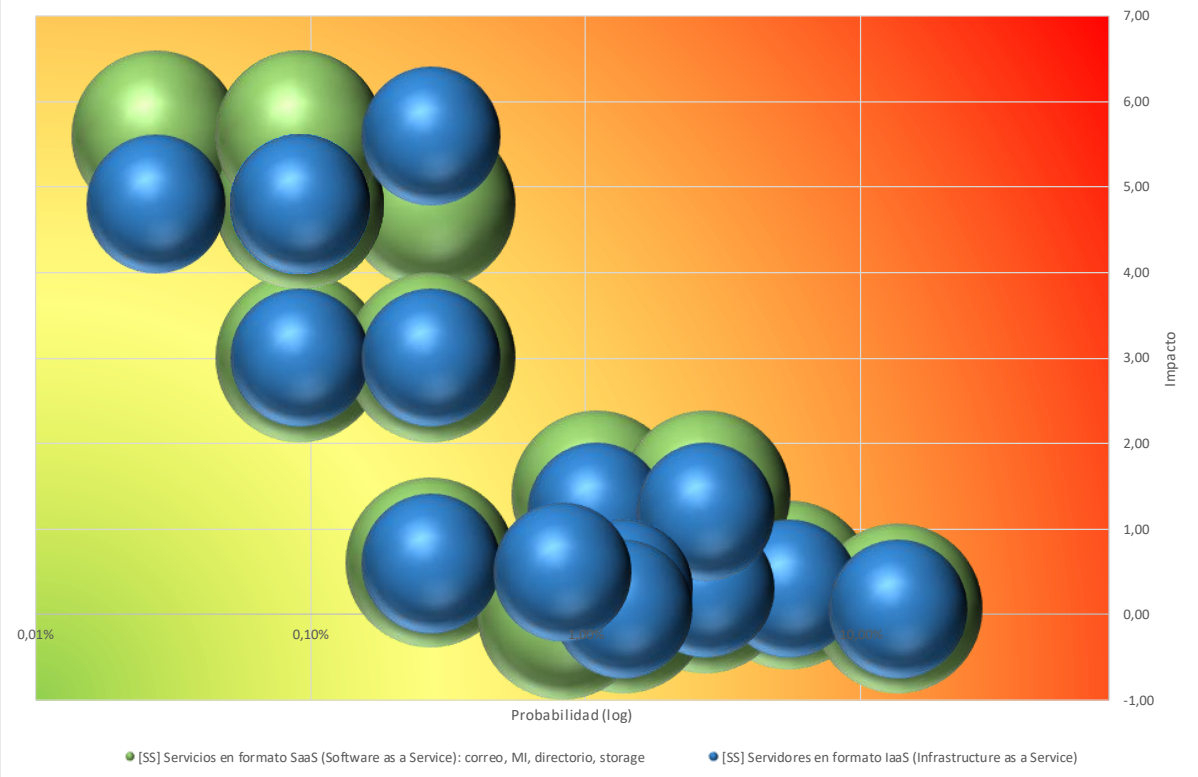


Imagen 35: Riesgos en Servicios Auxiliares

6.3.8 Equipamiento Auxiliar

- [Media] CD-Rom, DVD, Memoria USB
- [Media] Documentación en formato papel
- [AUX] Destructora de documentos
- [AUX] Sistema de cableado
- [AUX] UPS, Generadores eléctricos, Equipo de clima, etc.

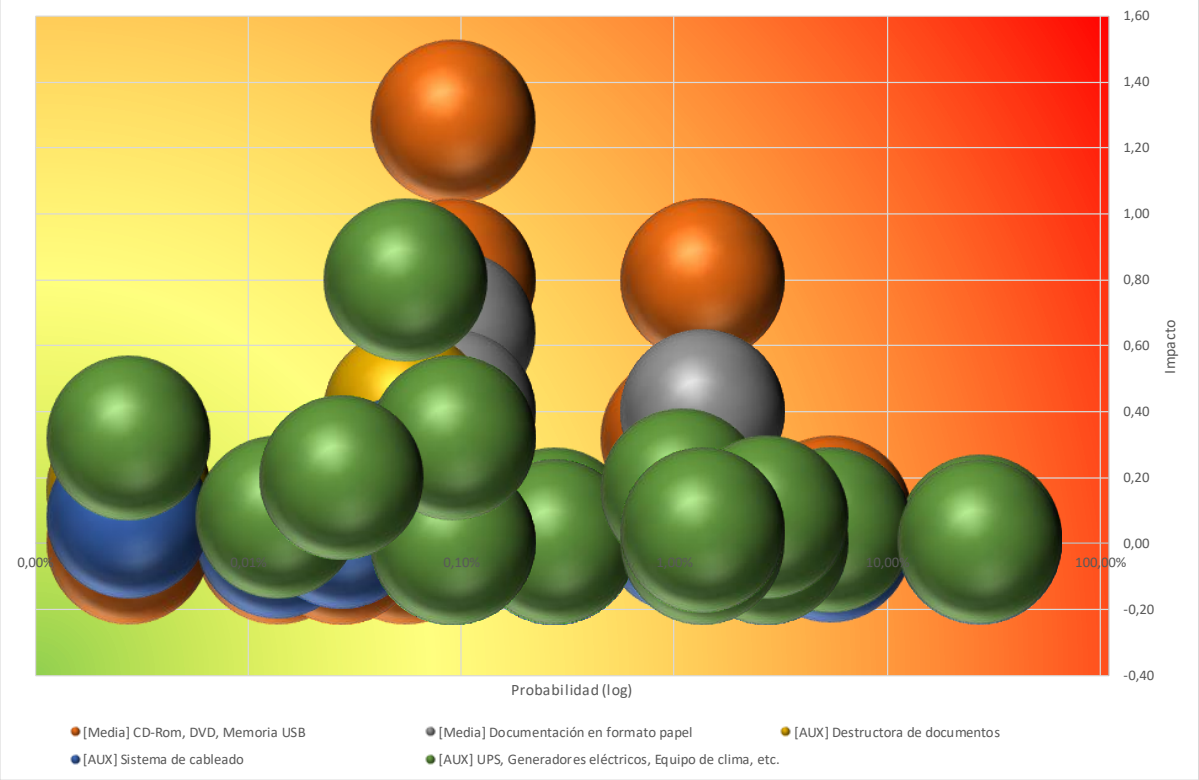


Imagen 36: Riesgos en Equipamiento Auxiliar

6.3.9 Personal

- [P] Administrador de comunicaciones
- [P] Administrador de seguridad
- [P] Administrador de sistemas
- [P] Usuarios

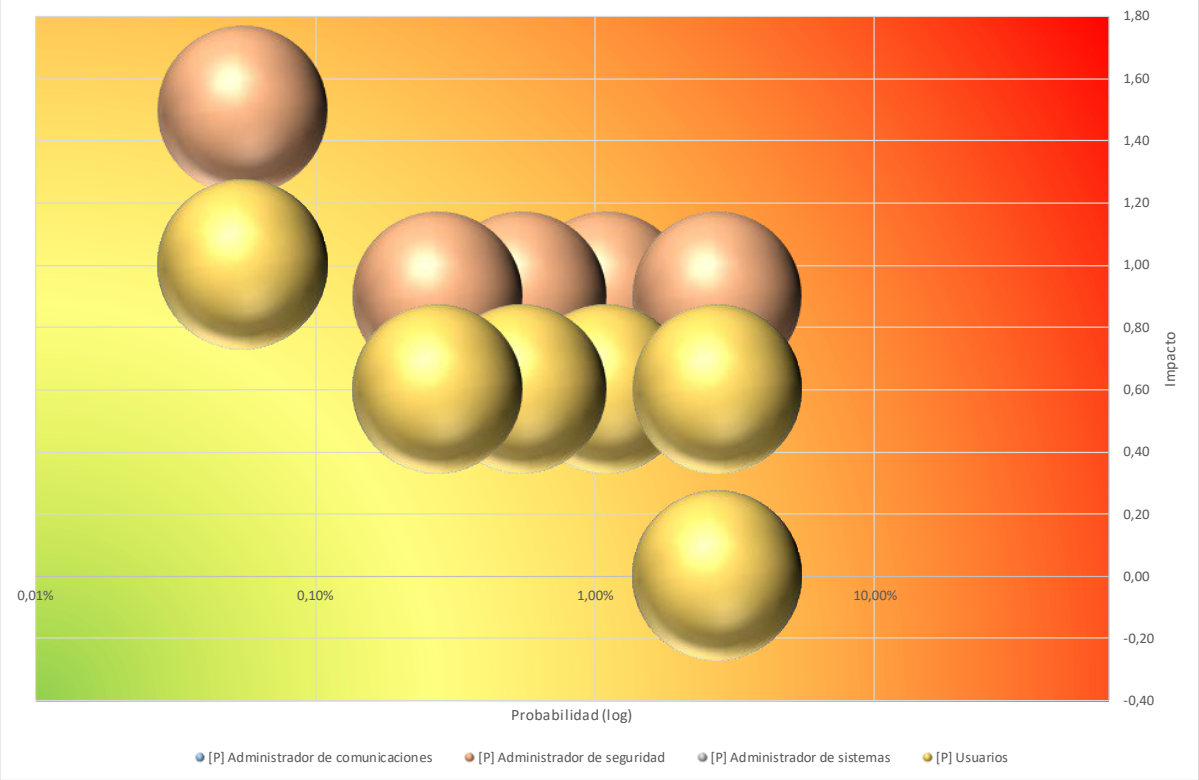
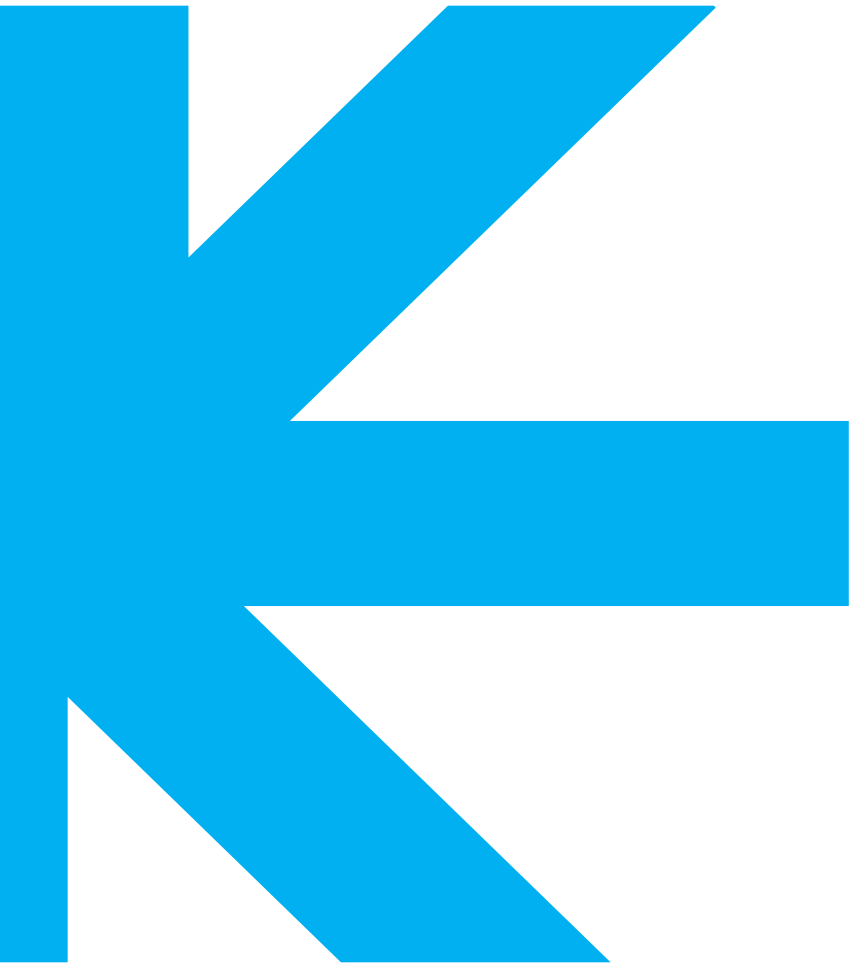


Imagen 37: Riesgos en Personal

6.4 Índice de Imágenes y Tablas



Edgar Muñoz Mercader

Máster Universitario de Seguridad de las Tecnologías de la Información y de las Comunicaciones

Universitat Oberta de Catalunya

e-mail: emunozmer@uoc.edu

edgar.munoz77@gmail.com