ANÁLISIS Y GESTIÓN DE RIESGOS A LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA CELUTEL SAS. EN LA CIUDAD DE SINCELEJO - SUCRE

JOSÉ LUIS PIEDRAHITA TATIS
MOSHE AARON BOSSA CASTRO

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS DE TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
COROZAL-SUCRE
2017

ANÁLISIS Y GESTIÓN DE RIESGOS A LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA CELUTEL SAS. EN LA CIUDAD DE SINCELEJO - SUCRE

JOSÉ LUIS PIEDRAHITA TATIS
MOSHE AARON BOSSA CASTRO

MONOGRAFÍA PARA OPTAR POR EL TÍTULO:
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
COROZAL-SUCRE
2017

Nota de Aceptación

_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

CONTENIDO

	Pág.
INTRODUCCIÓN	11
1. PLANTEAMIENTO DEL PROBLEMA	12
1.2 FORMULACIÓN DEL PROBLEMA	12
2. JUSTIFICACIÓN	13
3. OBJETIVOS	14
3.1 OBJETIVO GENERAL	14
3.2 OBJETIVOS ESPECÍFICOS	14
4. MARCO REFERENCIAL	15
4.1 ANTECEDENTES	15
4.2 MARCO TEÓRICO	16
4.3 MARCO CONCEPTUAL	19
4.4 MARCO LEGAL	21
5. MARCO METODOLÓGICO	23
5.1 METODOLOGÍA DE INVESTIGACIÓN	23
5.1.1 POBLACIÓN Y MUESTRA	23
5.1.2 FUENTES DE RECOLECCIÓN DE INFORMACIÓN	23
5.2 METODOLOGÍA DE DESARROLLO	23
6. DESARROLLO DEL PROYECTO	25
6.1 DESCRIPCIÓN DEL ENTORNO DE APLICACIÓN DEL PROYECTO	25
6.2 INVENTARIO TECNOLÓGICO	25

6.3 IDENTIFICACIÓN DE ACTIVOS SEGÚN MAGERIT. 27

6.4 VALORACIÓN CUALITATIVA DE LOS ACTIVOS SEGÚN MAGERIT 30

6.5 IDENTIFICACIÓN DE LAS AMENAZAS SEGÚN MAGERIT 34

6.6 ESTIMACIÓN DEL RIESGO 48

6.6.1 IMPACTO POTENCIAL ACUMULADO 48

6.6.2 RIESGO POTENCIAL ACUMULADO 50

6.7 IDENTIFICACIÓN DE SALVAGUARDAS 55

7. CONCLUSIONES 60

8. RECOMENDACIONES 61

BIBLIOGRAFIA 62

ANEXOS 67

LISTA DE TABLAS

Pág.

Tabla 1. Estándares ISO **18**

Tabla 2. Inventario sistema de información CELUTEL S.A.S **25**

Tabla 3. Activos de información **26**

Tabla 4. Escala de valoración de las dimensiones **31**

Tabla 5. Valoración de activos por dimensión **31**

Tabla 6. Probabilidad de ocurrencia de una amenaza según ear/pilar **34**

Tabla 7. Criterios de Valoración del impacto **48**

Tabla 8. Resumen Riesgo acumulado del activo servidor **58**

LISTA DE FIGURAS

Pág.

Figura 1. Activos identificados en ear/pilar **29**

Figura 2. Valoración de activos en ear/pilar **33**

Figura 3. Amenazas sobre el activo BD_GENERAL **35**

Figura 4. Amenazas sobre el activo BD_CELSIS **36**

Figura 5. Amenazas sobre el activo EMAIL y S_INTERNET **37**

Figura 6. Amenazas sobre el activo SW_GENERAL LEDGER **37**

Figura 7. Amenazas sobre el activo PL_POLIEDRO **38**

Figura 8. Amenazas sobre el activo SW_CELSIS **38**

Figura 9. Amenazas sobre el activo SQL_SERVER **39**

Figura 10. Amenazas sobre el activos SO, OFFICE y AV **39**

Figura 11. Amenazas sobre el activo PC_S **40**

Figura 12. Amenazas sobre el activo PC **40**

Figura 13. Amenazas sobre el activo PRINT **41**

Figura 14. Amenazas sobre el activos SCAN **41**

Figura 15. Amenazas sobre el activos SWITCH **42**

Figura 16. Amenazas sobre el activos CONMUTADOR **42**

Figura 17. Amenazas sobre el activos CAMARA **43**

Figura 18. Amenazas sobre los activos ADSL y TEL **43**

Figura 19. Amenazas sobre el activo [LAN] **44**

Figura 20. Amenazas sobre el activo [WIFI] **44**

Figura 21. Amenazas sobre el activos [UPS_SERVIDOR] **45**

Figura 22. Amenazas sobre el activo [ADSL] **45**

Figura 23. Amenazas sobre el activo [OFFICINA] **45**

Figura 24. Amenazas sobre el activos [IS] y [USER_OP_CONT] **46**

Figura 25. Amenazas sobre los activos [USER_OP_BOD], [USER_OP_CAJA] y [USER_OP_VENT] **46**

Figura 26. Impacto potencial acumulado de los activos de la empresa CELUTEL SAS **49**

Figura 27. Niveles de criticidad ear/pilar **50**

Figura 28. Riesgo potencial acumulado de los activos de la empresa CELUTEL SAS **51**

Figura 29. Salvaguardas en ear/pilar **56**

Figura 30. Salvaguardas para riesgos de activos de CELUTEL SAS ear/pilar **58**

LISTA DE ANEXOS

Pág.

Anexo A **67**

Anexo B **68**

Anexo C **75**

INTRODUCCIÓN

Uno de los bienes más representativos de una empresa es la información, en la actualidad son pocas las empresas que aún no tienen este bien protegido, y se debe a que desconocen los peligros que corren por el mal manejo de la información o por no tener un sistema de información protegido y optimizado, esto se convierte en una gran falencia debido a que en el presente existen muchas formas en las cuales una persona con conocimiento en herramientas informáticas, podría vulnerar la seguridad y extraer la información que posea una empresa, siendo este el mejor de los casos, ya que podrían presentarse casos más graves donde no sea solo una extracción de información sino que podría ser una eliminación de la misma, lo que traería graves consecuencias para la empresa, por este motivo es fundamental implementar auditorías a la seguridad informática y al manejo de la información en todas las empresas, para ello existen metodologías que se pueden usar para mitigar todas esas falencias presentadas en un sistema de seguridad.

La metodología Magerit ofrece una herramienta poderosa para el análisis y la gestión de riesgos en los sistemas de información, esta metodología permite mitigar los riesgos que la implementación de tecnologías de la información puedan acarrear, con su implementación se logra tener sistemas de información más seguros y eficientes, además de contar con planes de contingencia en el caso de presentarse una eventualidad prevista durante el análisis realizado a cualquier empresa.

Con la implementación de Magerit en CELUTEL SAS, se lograra identificar en primera instancia las vulnerabilidades presentes, las cuales en este momento son muy grandes, entre ellas se destacan no contar con Backus externos para las bases de datos, y la exposición de los equipos servidores a el acceso por cualquier empleado de la empresa, sin mencionar que se carece de una estructura organizativa para el manejo de la información, una vez marcadas todas estas vulnerabilidades se procede a su valoración y clasificación, este proceso brindara a CELUTEL SAS, bases solidadas para implementar los correctivos y los planes de contingencia posibles para el manejo de cualquier riesgo presentado.

1. PLANTEAMIENTO DEL PROBLEMA

En el presente la información es un bien fundamental de toda empresa, el cual se encuentra constantemente expuesto a daños por la naturaleza o por agentes humanos, la importancia de este bien radica en su utilización, es decir este bien en la mayoría de los casos es el motor de la empresa, debido a que mantiene el registro de las operaciones, la contabilidad, los inventarios y los clientes, por tal razón una pérdida de este bien, acarrea a la empresa un gasto enorme de dinero o en el peor de los casos perdidas irrecuperables, como podría ser la perdida completa de la base de datos de los registros de venta, o peor aún la perdida de la información contable donde se registren carteras, saldos pendientes y un detallado de donde está el dinero de la empresa.

Actualmente CELUTEL SAS se encuentra expuesta a todos los riesgos antes mencionados, no posee planes de contingencia y es mas no tiene siquiera una valoración de los activos con los que cuenta, lo que la ubica entre las empresas con mayor riesgos en su sistema de información, es de destacar que la información en CELUTEL SAS es fundamental para el desarrollo de las actividades diarias, debido a que se deben registrar ventas de celulares como también venta de servicios (planes de celulares), además los registros contables de las entregas a los subdistribuidores y actualizaciones de carteras, y en caso de pérdida generarían un desastre en el funcionamiento normal de la empresa y perdidas monumentales.

Por tal motivo es fundamental aplicar a CELUTEL SAS, Magerit e ISO 27001 y reducir con ello los riesgos, crear planes de contingencia y sobre todo incrementar la seguridad de su sistema de información a través de políticas de seguridad, antes de que se presenten nuevas pérdidas como la presentada en el año 2012 año en el cual el servidor de bases de datos tubo daños en el único disco duro que tenía, lo que generó una perdida irrecuperable de información y gran conmoción en toda la empresa y sus filiales.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo identificar y tratar los riesgos que exponen la seguridad de la información en la empresa CELUTEL SAS, en la ciudad de Sincelejo-Sucre, con el fin implementar un sistema de gestión de seguridad que mitigue los riesgos posibles?

2. JUSTIFICACIÓN

Magerit es una metodología para auditorias de sistemas informáticos más utilizada en el mundo, mediante su implementación se logra identificar plenamente los riesgos a los que está expuesto un bien de una empresa y además permite implementar salvaguardas o medidas de contingencia y manejo de todos esos riesgos identificados, estos factores la convierten en una metodología sólida y su implementación no es muy compleja.

ISO 27001, es la norma emitida por la organización internacional de normas (ISO), cuya finalidad es la implementación de la gestión de la seguridad informática, su principal objetivo es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa, todo ello a través del análisis de riesgo que en este caso será realizado con Magerit.

Actualmente la situación de CELUTEL SAS, no es del todo grata, el sistema de información en general se encuentra expuesto a todos los factores posibles de daño, además la seguridad es inexistente, los accesos a información crítica son completamente abiertos a todo el personal laboral de la empresa y no solo a ellos también a una gran mayoría de clientes los cuales pueden circular por la empresa sin un control para tal evento. Entre los inconvenientes presentados se destacan virus en los sistemas, perdida de información por daño en los discos duros (apagones imprevistos), los cuales generan gastos no solo de dinero sino de mano de obra de los empleados al tener que reconstruir los registros digitales a partir de los archivos físicos dado el caso que se localicen, en muchos casos no hay registro físico de las operaciones lo que genera una perdida irrecuperable de la información.

Al aplicar Magerit e ISO 27001 a CELUTEL SAS, se tendrá un panorama claro sobre todos los bienes con los que cuenta la empresa, estos bienes serán catalogados y valorados, para posterior mente identificar los riesgos a los cuales están expuestos, logrando con ello tener conciencia de que tan vulnerable es el sistema de información con el que cuenta la empresa, una vez catalogados se procede a designar los salvaguardas que serán utilizados para el manejo de cada uno de los riesgos identificados y además todas las políticas de seguridad necesarias para la gestión de la seguridad informática, llevando así a CELUTEL SAS, a la obtención de un sistema de información sólido, y mucho más seguro que el actual, previniendo así, daños graves y perdida de información que puede ser vital para el desarrollo de las actividades diarias de la empresa, como también la perdida de dinero ocasionada por el daño de los bienes con los que actualmente se cuenta.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Fortificar el sistema de información de la empresa CELUTEL SAS, de Sincelejo Sucre, mediante la aplicación del análisis y gestión de riesgos de la seguridad de la información utilizando la metodología MAGERIT v3 y la norma ISO 270001:2013.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar y clasificar los activos con los que cuenta la CELUTEL SAS, en su sistema de información

- Aplicar el análisis de riesgo, identificando, cuantificando y definiendo las amenazas posibles en los activos del sistema de información de CELUTEL SAS.

- Gestionar los riegos, definir salvaguardas, que mitiguen, eviten, impidan o vuelvan manejable un riesgo posible en la empresa CELUTEL SAS.

- Realizar un plan de políticas de seguridad enmarcadas por la norma ISO 27001 para la gestión de la seguridad de la información de la empresa CELUTEL SAS.

4. MARCO REFERENCIAL

4.1 ANTECEDENTES

La necesidad subyacente de este proyecto es la realización del análisis y la gestión de la seguridad de la información en la empresa CELUTEL SAS, basado en los percances presentados en los distintos sectores de la misma, para llevar a cabo este proceso es necesario conocer a fondo los antecedentes presentes en lo relacionado con los sistemas de gestión de seguridad informática.

Dentro de los estándares y metodologías establecidas para analizar los riesgos y gestionar la seguridad, se destacan dos muy importantes, el estándar o norma ISO 27001 y la metodología Magerit v3.

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2[1].

Esta norma es la más utilizada en la actualidad para la implementación de los SGSI, debido a su estructura sólida y bien definida, la cual se centra en 4 peldaños, los cuales son: manual de seguridad, procedimientos, instrucciones cheklist formularios y registros.

La norma ISO 27001:2013 aunque muy completa se apoya en el análisis de riesgo y la mejor metodología para realizar este análisis de riesgo Magerit, la cual se define como “la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno. Actualizada en 2012 en su versión 3[2], por lo cual su implementación es de mucha utilidad al momento de evaluar los activos y a los riesgos que se expone una empresa, además nos permite diseñar y crear salvaguardas para el tratamiento de los riesgos posibles.

[1] Norma 20071 https://advisera.com/27001academy/es/que-es-iso-27001/

[2] Metodología Magerit https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WLYPsdI1_IU

Para aplicar la metodología de la mejor forma es necesario utilizar el aplicativo EAR/PILAR. Las herramientas EAR (entorno de análisis de riesgo) soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit[3]. Lo que la convierte en una herramienta muy útil al momento de realizar un análisis de los riesgos posibles en los activos y crear para ellos salvaguardas, lo que facilitara las labores en una empresa, en este caso CELUTEL SAS.

4.2 MARCO TEÓRICO

Análisis de riesgo: mediante el análisis de riesgo es posible obtener un estado real de los riesgos en una entidad, uno de sus propósitos principales es la identificación puntual de los principales riesgos denomínense estos fallos de infraestructura, planta personal y desastres naturales, los cuales al momento de presentarse generarían problemas a las operaciones normales de la entidad ocasionando caos, además de la identificación del riesgo se aplica también una priorización de medidas que puedan disminuir la probabilidad de ocurrencia de estos riesgos, y en caso de que sea materializado se diseñan salvaguardas los cuales al ser implementados mitigan el impacto generado por el riesgo presentado.

Magerit: es la metodología de análisis y gestión de riesgo más utilizada en las empresas en las cuales su funcionamiento se encuentra centrado en el manejo de tecnologías informáticas para su quehacer diario, esta metodología proporciona ciertos procedimientos los cuales permiten la identificación y valoración de los activos con los cuales cuenta una empresa y además permite identificar el riesgo al cual está expuesto cada uno de ellos, presentando para cada riesgo una forma de mitigarlo en caso de que este se materialice. La metodología Magerit cuenta con 3 libros los cuales trabajan a detalle la forma en la cual se debe realizar el análisis y gestión de riesgos dentro de un sistema de información en una empresa.

Sistema de información: conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio. Teniendo muy en cuenta el equipo computacional necesario para que el sistema de información pueda operar y el recurso humano que interactúa con el Sistema de Información, el cual está formado por las personas que utilizan el sistema[4].

[3] Herramientas ear/pilar, http://www.ar-tools.com/es/index.html

[4] Armando Duany Dangel (24 de Feb. de 2010). "Sistemas de Información". [En línea] Dirección URL: http://www.econlink.com.ar/sistemas-informacion/definicion (Consultado el 22 de Feb. de 2017)

Sistema de gestión de la seguridad de la información (SGSI): según ISO 27001 un sistema de gestión de la información cosiste fundamentalmente en la preservación de la confidencialidad, la integridad y la disponibilidad, que pueda tener la información dentro de una empresa, como también todos los sistemas que se vean vinculados en el manejo de tal información.

Se debe entender por información todos los datos con los cuales cuenta una empresa, y los cuales le dan la esencia a su funcionamiento, es decir todos los datos relevantes o no con los cuales cuenta la empresa para el desarrollo de sus actividades diarias y el mantenimiento de sus registros a través de los años.

Con la implementación de un SGSI en una empresa se crea una herramienta que permite tener un panorama claro sobre el estado de los sistemas informáticos, esto se logra con la combinación de los recursos disponibles dentro de la empresa, esta combinación presentada entre los recursos humanos y técnicos, proporciona métodos precisos para el manejo de todo riesgo, y con la unión a esta combinación de la parte administrativa de la empresa la cual se encargaría de garantizar que esos métodos sean acogidos por toda la planta de personal, se lograría tener un sistema de información en el cual los riesgos se mantendrán siempre en un nivel bajo de materialización, lo que se verá reflejado en el funcionamiento estable y eficiente de la empresa

Normas ISO sobre gestión de seguridad de la información: las normas ISO son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) que se encargan de establecer estándares y guías relacionados con sistemas de gestión y aplicables a cualquier tipo de organización internacionales y mundiales, con el propósito de facilitar el comercio, facilitar el intercambio de información y contribuir a la transferencia de tecnologías[5].

En concreto la familia de normas ISO/IEC 27000 son un conjunto de estándares de seguridad (desarrollados o en fase de desarrollo) que proporciona un marco para la gestión de la seguridad.

[5]Normas ISO sobre gestión de seguridad de la información, http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html

Dentro de las normas ISO dedicadas a la gestión de la seguridad de la información se destacan:

Tabla 1. Estándares ISO/IEC

Norma	Descripción
ISO/IEC 27000	Vocabulario estándar para el SGSI para todas las normas de la familia. Se encuentra en desarrollo actualmente.
ISO/IEC 27001	Certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005.
ISO/IEC 27002	*Information technology - Security techniques - Code of practice for information security management*. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es un **código de buenas prácticas** para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007.
ISO/IEC 27003	Directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Publicada el 1 de febrero del 2010, No está certificada actualmente.
ISO/IEC 27004	Métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre del 2009, no se encuentra traducida al español actualmente.
ISO/IEC 27005	Normativa dedicada exclusivamente a la gestión de riesgos en seguridad de la información. Proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada a la actual British Standard BS 7799 parte 3. Publicada en junio de 2008.
ISO/IEC 27006	Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma específica requisitos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.
ISO/IEC 27007	Guía para auditar al SGSI. Se encuentra en preparación.
ISO/IEC 27799:2008	Guía para implementar ISO/IEC 27002 en la industria de la salud.

Ear/Pilar: entorno de análisis de riesgo, esta es una herramienta que permite realizar el análisis de riesgo mediante la utilización de la metodología Magerit, esta herramienta es muy intuitiva y ofrece muchas salvaguardas para el manejo del riesgo materializado.

4.3 MARCO CONCEPTUAL

Activos: son todos los elementos que conforman el sistema de información (hardware, software, instalaciones, los servicios prestados, documentos)

Amenaza: son inconvenientes que puedan presentarse sobre los activos de una empresa y los cuales pueden ser generados por fenómenos de la naturaleza o por la planta de personal de la empresa.

Vulnerabilidad: debilidad que posea un activo y que puede verse afectada por una amenaza, convirtiendo esa situación en un riesgo de seguridad en la información.

Impacto: consecuencias producidas por la materialización de un riesgo sobre un activo.

Riesgo: Es la probabilidad de que ocurra un evento y sus consecuencias negativas ocasionando daños o perdidas.

Disponibilidad: capacidad para mantener la información siempre utilizable o que su recuperación sea pronta.

Confidencialidad: La información solo puede ser consultada y modificada por personal autorizado.

Integridad: Que la información no haya sido modificada, es decir que sea igual a los datos de origen.

Desastres de origen natural: Accidentes causados por fenómenos naturales (terremotos, inundaciones, huracanes…)

Desastres de origen industrial: Accidentes causados por desastres industriales (fallos eléctricos, explosiones…)

Errores y fallos no intencionados: Estos accidentes normalmente son causados por personal con permisos para acceder al sistema y causan fallas en el sistema por error o por omitir algunos procesos.

Ataques intencionados: Este tipo de ataques es causado por personal con acceso a la información y atacan el sistema con intenciones de conseguir un beneficio propio.

Arquitectura del sistema: Se estructura el sistema demostrando su arquitectura interna buscando relacionarlos con el exterior.

Datos o Información: Son la base fundamental de la organización es de tipo abstracto el cual es almacenado en equipos (comúnmente almacenados en bases de datos) el cual es traslado por diferentes medios hacia otros lugares (memorias USB, internet, discos externos).

Servicios: Su función es complacer la necesidad de los usuarios que utilicen los servicios del sistema.

Equipamiento Informático: Aquellos medio materiales, físicos, encargados de hacer funcionar los servicios prestados por la organización.

Redes de comunicaciones: Encargada de enviar y recibir la información de la organización o terceros.

Soportes de información: Aquellos dispositivos físicos donde se almacena información por largos periodos de tiempo.

Equipamiento auxiliar: Hace referencia aquellos equipos que brindan apoyo a los equipos de información.

Instalaciones: Lugar donde están ubicados los equipos de información y comunicaciones**.**

Personal: Todo aquel conjunto de personas que trabaja sobre los equipos de información o comunicaciones.

4.4 MARCO LEGAL

Ley 1581 de 2012 (Protección de Datos Personales): Es una ley que complementa la regulación vigente para la protección del derecho fundamental que tiene todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación[6].

Ley 1341 del 30 de julio de 2009: Con la que se busca darle a Colombia un marco normativo para el desarrollo del sector de Tecnologías de Información y Comunicaciones (TIC), promueve el acceso y uso de las TIC a través de la masificación, garantiza la libre competencia, el uso eficiente de la infraestructura y el espectro, y en especial, fortalece la protección de los derechos de los usuarios.
Ley 1273: El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

[6]MINTIC. El Congreso de Colombia Decreta. Disponible en: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdff

Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Decisión 352 de la C.A.N: Las disposiciones de la presente Decisión tienen por finalidad reconocer una adecuada y efectiva protección a los autores y demás titulares de derechos, sobre las obras del ingenio, en el campo literario, artístico o científico, cualquiera que sea el género o forma de expresión y sin importar el mérito literario o artístico ni su destino.

Decreto 460 de 1995: Por el cual se reglamenta el Registro Nacional del Derecho de Autor y se regula el Depósito Legal

5. MARCO METODOLÓGICO

5.1 METODOLOGÍA DE INVESTIGACIÓN

Esta investigación está enfocada en analizar el estado de todos los activos con los cuales cuenta CELUTEL SAS, teniendo en cuenta los aspectos definidos por la norma ISO 27001 y sus tres elementos fundamentales confidencialidad, integridad y disponibilidad, aplicado a su sistema de información actual, lo cual le da un enfoque de tipo cuantitativo a esta investigación.

5.1.1 Población y muestra: la población que se utilizara durante el desarrollo de este proyecto serán todos empleados de la empresa CELUTEL SAS, en su sede principal.

Para la muestra serán tomados todos empleados de la empresa debido a que todos ellos tienen contacto con el sistema de información, actualmente la empresa tiene en su sede principal 16 empleados los cuales funcionaran como la muestra para el desarrollo del proyecto

5.1.2 Fuentes de recolección de información: los métodos que se utilizaran para la recolección de datos, serán, observación directa, entrevistas y listas de chequeo para conocer a profundidad las falencias dentro de la organización estas se aplicaran a los usuarios y equipos del sistema de información dentro de la muestra.

5.2 METODOLOGÍA DE DESARROLLO

Objetivo 1: Identificar y clasificar los activos con los que cuenta la CELUTEL SAS, en su sistema de información

- ✓ Realizar visita a la empresa para conocer a detalle todos los activos con los que cuenta CELUTEL SAS.

- ✓ Clasificar los activos con los que cuenta la empresa teniendo en cuenta estado y ubicación además del acceso a ellos por el personal.

Objetivo 2: Aplicar el análisis de riesgo, identificando, cuantificando y definiendo los riegos posibles en los activos del sistema de información de CELUTEL SAS.

- ✓ Utilizar una lista de chequeo basados en el estándar Magerit para conocer las amenazas posibles sobre los activos en la empresa y así determinar su nivel de riesgo.

Objetivo 3: Gestionar los riegos, definir salvaguardas, que mitiguen, eviten, impidan o vuelvan manejable un riesgo posible en la empresa CELUTEL SAS.

- ✓ Utilizar el análisis arrojado por EAR/PILAR para consolidación de los salvaguardas pertinentes a cada uno de los riesgos potenciales.

Objetivo 4: Realizar un manual con las políticas de seguridad definidas por la norma ISO 27001 para la gestión de la seguridad de la información de la empresa CELUTEL SAS.
.

- ✓ Establecer políticas de seguridad para el manejo de los posibles riesgos

- ✓ Crear el plan de políticas de seguridad necesarias para CELUTEL SAS.

- ✓ Socialización del Plan de políticas de seguridad en la empresa CELUTEL SAS

6. DESARROLLO DEL PROYECTO

6.1 DESCRIPCIÓN DEL ENTORNO DE APLICACIÓN DEL PROYECTO

CELUTEL SAS, distribuidor autorizado de CLARO (telefonía celular), se encuentra ubicada en Sincelejo, departamento de Sucre, en el parque bolívar de la ciudad, en la dirección Calle 20 #19 - 61 Centro

6.2 INVENTARIO TECNOLÓGICO

Tabla 2. Inventario sistema de información CELUTEL SAS

TIPO DE ACTIVO	ACTIVO	SERVICIO	SISTEMA OPERATIVO	CANTIDAD
Tangible	Switch Dlink	Intercomunicación de la red LAN		1
Tangible	Red telefónica ADSL	Intercomunicación entre extensiones		1
Tangible	Red de cableado estructurado	Interconectividad de red		1
Tangible	Servidor HP ProLiant DL380p Gen8, procesador Intel® Xeon® E5-2600 v2; Memoria RAM 8 GB Discos duros (2) 1TB (espejo)		Windows server 2012	1
Tangible	Ups NICOMAR 2KVA	Sistema de alimentación ininterrumpida		1
Tangible	Computadores de escritorio Hp		Windows 7 de 64 Bits Office 2010 Antivirus	15

			Microsoft Security Essentials	
Tangible	Computador portátil Hp Procesador Core i5 Memoria Ram,4GB Disco duro 1 TB		Windows 7 de 64 Bits Antivirus (Microsoft Security Essentials)	1
Tangible	Impresora térmica			1
Tangible	Impresora láser			4
Tangible	Escáner			2
Tangible	Cámaras de vigilancia	Sistema de circuito cerrado de seguridad		8
Tangible	Teléfonos	Comunicación con el exterior e intercomunicación		6
Intangible	Servicio de internet	Navegación en internet		1
Intangible	Base de datos general ledger	Almacena información contable y financiera(general ledger)	Instalado sobre plataforma Windows Server	1
Intangible	Bases de datos celsis	Registro de ventas y clientes, inventario de equipos	Instalado sobre plataforma Windows Server	1
Intangible	Software General ledger	Manejo contable, financiero y de almacén	Instalado sobre plataforma Windows 7	6
Intangible	Software CELSIS	Sistema de administración de ventas	Instalado sobre plataforma Windows 7	1

6.3 IDENTIFICACIÓN DE ACTIVOS SEGÚN MAGERIT.

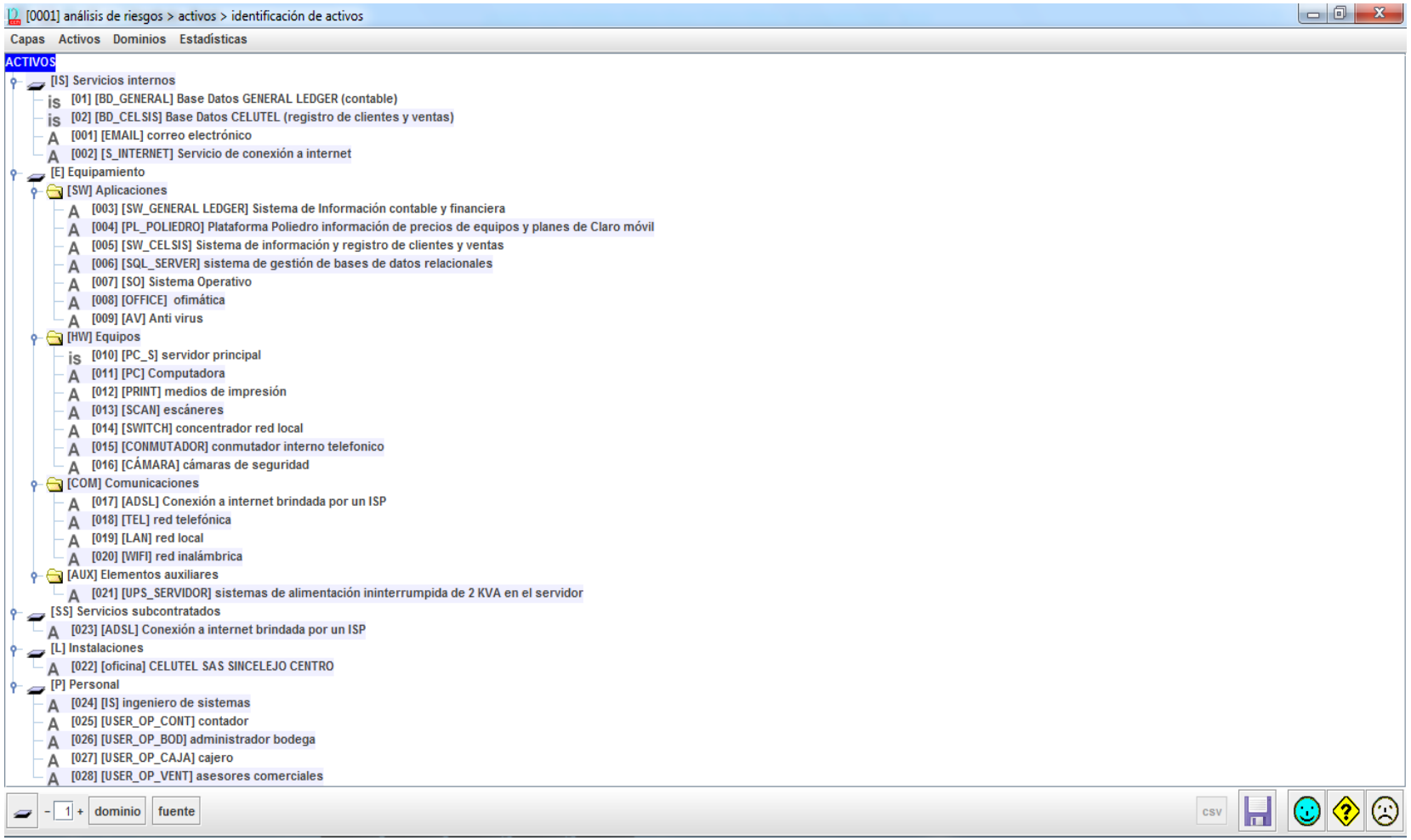
Los activos presentes en la empresa CELUTEL SAS, son identificados y clasificados tomando como base el Libro II de la metodología MAGERIT versión 3, en donde nos presenta el catálogo de elementos:

Tabla 3: Activos de información

TIPO	NOMBRE DEL ACTIVO
DATOS / INFORMACIÓN	1. [BD_GENERAL] Base Datos GENERAL LEDGER (contable)
	2. [BD_CELSIS] Base Datos CELUTEL (registro de clientes)
SERVICIOS	3. [EMAIL] correo electrónico @celutel.com.co
	4. [S_INTERNET] Servicio de conexión a internet
APLICACIONES	5. [SW_GENERAL LEDGER] Sistema de Información contable y financiera
	6. [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil
	7. [SW_CELSIS] Sistema de información y registro de clientes y ventas
	8. [SQL_SERVER] sistema de gestión de bases de datos relacionales
	9. [SO] Sistema Operativo
	10. [OFFICE] ofimática
	11. [AV] Anti virus
EQUIPAMIENTO INFORMÁTICO	12. [PC_S] servidor principal
	13. [PC] Computadora
	14. [PRINT] medios de impresión
	15. [SCAN] escáneres
	16. [SWITCH] concentrador red local
	17. [CONMUTADOR] conmutador interno telefónico
	18. [CÁMARA] cámaras de seguridad
REDES DE COMUNICACIONES	19. [ADSL] Conexión a internet brindada por un ISP
	20. [TEL] red telefónica

	21. [LAN] red local
	22. [WIFI] red inalámbrica
EQUIPAMIENTO AUXILIAR	23. [UPS] sistemas de alimentación ininterrumpida de 2 KVA en el servidor
INSTALACIONES	24. [oficina] CELUTEL SAS SINCELEJO CENTRO
PERSONAL	25. [IS] ingeniero de sistemas
	26. [USER_OP_CONT] contador
	27. [USER_OP_BOD] administrador bodega
	28. [USER_OP_CAJA] cajero
	29. [USER_OP_VENT] asesores comerciales

Figura 1: activos identificados en ear/pilar



6.4 VALORACIÓN CUALITATIVA DE LOS ACTIVOS SEGÚN MAGERIT

Para realizar el proceso de valoración de activos de acuerdo a la metodología MAGERIT Versión 3; se usa las siguientes dimensiones[7]:

- [D] Disponibilidad: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]

- [I] Integridad de los datos: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]

- [C] Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]

- [A] Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]

- [T] Trazabilidad: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]

"Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión".

[7]Tomado de: 2012_Magerit_v3_libro2_catálogo de elementos_es_NIPO_630-12-171-8.

Tabla 4. Escala de valoración de las dimensiones

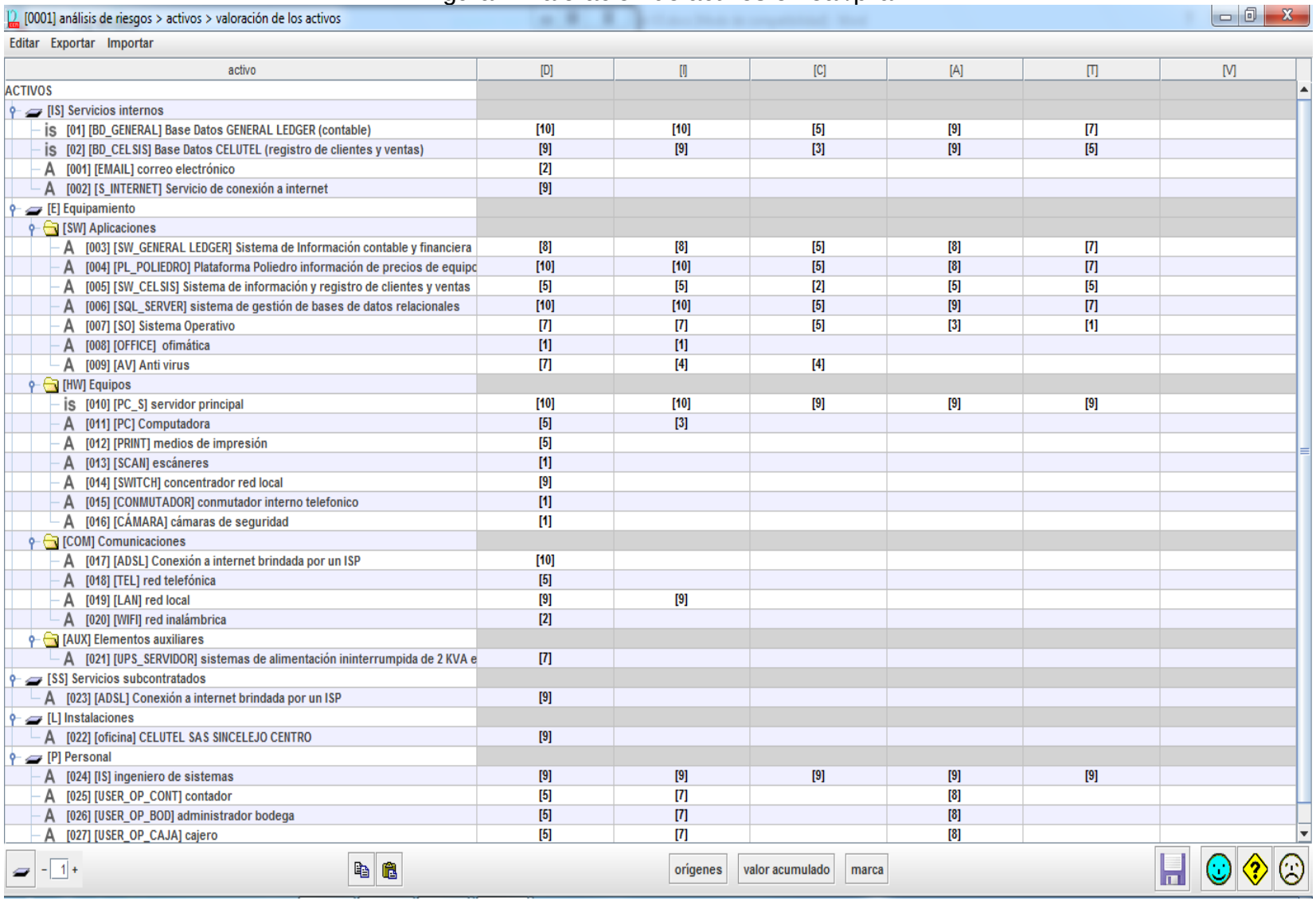
VALOR		CRITERIO
10	EXTREMO	Daño extremadamente grave
9	MUY ALTO	Daño muy grave
6-8	ALTO	Daño grave
3-5	MEDIO	Daño importante.
1-2	BAJO	Daño menor.
0	DESPRECIABLE	Irrelevante a efectos prácticos.

Tabla 5. Valoración de activos por dimensión

ACTIVOS	**DIMENSIONAMIENTO**				
DATOS / INFORMACIÓN	**D**	**I**	**C**	**A**	**T**
[BD_GENERAL] Base Datos GENERAL LEDGER (contable)	10	10	5	9	7
[BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	9	9	3	9	5
Servicios	**D**	**I**	**C**	**A**	**T**
[EMAIL] correo electrónico @celutel.com.co	2				
[S_INTERNET] Servicio de conexión a internet	9				
APLICACIONES	**D**	**I**	**C**	**A**	**T**
[SW_GENERAL LEDGER] Sistema de Información contable y financiera	8	8	5	8	7
[PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	10	10	5	9	7
[SW_CELSIS] Sistema de información y registro de clientes y ventas	5	5	2	5	5
[SQL_SERVER] sistema de gestión de bases de datos relacionales	10	10	5	9	7
[SO] Sistema Operativo	7	7	5	3	1
[OFFICE] ofimática	1	1			
[AV] Anti virus	7	4	4		4
EQUIPAMIENTO INFORMÁTICO	**D**	**I**	**C**	**A**	**T**
[PC_S] servidor principal	10	10	9	9	9

[PC] Computadora	5	3			
[PRINT] medios de impresión	5				
[SCAN] escáneres	1				
[SWITCH] concentrador red local	9				
[CONMUTADOR] conmutador interno telefónico	1				
[CÁMARA] cámaras de seguridad	1				
COMUNICACIONES	**D**	**I**	**C**	**A**	**T**
[ADSL] Conexión a internet brindada por un ISP	10				
[TEL] red telefónica	5				
[LAN] red local	9	9	9		
[WIFI] red inalámbrica	2				
Equipos Auxiliares	**D**	**I**	**C**	**A**	**T**
[UPS_SERVIDOR] sistemas de alimentación ininterrumpida de 2 KVA en el servidor	7				
INSTALACIONES					
[oficina] CELUTEL SAS SINCELEJO CENTRO	10				
Personal	**D**	**I**	**C**	**A**	**T**
[IS] ingeniero de sistemas	9	9	9	9	9
[USER_OP_CONT] contador	5	7		8	
[USER_OP_BOD] administrador bodega	5	7		8	
[USER_OP_CAJA] cajero	5	7		8	
[USER_OP_VENT] asesores comerciales	5			8	

Figura 2: valoración de activos en ear/pilar



activo	[D]	[I]	[C]	[A]	[T]	[V]
ACTIVOS						
[IS] Servicios internos						
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[10]	[10]	[5]	[9]	[7]	
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[9]	[9]	[3]	[9]	[5]	
[001] [EMAIL] correo electrónico	[2]					
[002] [S_INTERNET] Servicio de conexión a internet	[9]					
[E] Equipamiento						
[SW] Aplicaciones						
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[8]	[8]	[5]	[8]	[7]	
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipc	[10]	[10]	[5]	[8]	[7]	
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[5]	[5]	[2]	[5]	[5]	
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[10]	[10]	[5]	[9]	[7]	
[007] [SO] Sistema Operativo	[7]	[7]	[5]	[3]	[1]	
[008] [OFFICE] ofimática	[1]	[1]				
[009] [AV] Anti virus	[7]	[4]	[4]			
[HW] Equipos						
[010] [PC_S] servidor principal	[10]	[10]	[9]	[9]	[9]	
[011] [PC] Computadora	[5]	[3]				
[012] [PRINT] medios de impresión	[5]					
[013] [SCAN] escáneres	[1]					
[014] [SWITCH] concentrador red local	[9]					
[015] [CONMUTADOR] conmutador interno telefonico	[1]					
[016] [CÁMARA] cámaras de seguridad	[1]					
[COM] Comunicaciones						
[017] [ADSL] Conexión a internet brindada por un ISP	[10]					
[018] [TEL] red telefónica	[5]					
[019] [LAN] red local	[9]	[9]				
[020] [WIFI] red inalámbrica	[2]					
[AUX] Elementos auxiliares						
[021] [UPS_SERVIDOR] sistemas de alimentación ininterrumpida de 2 KVA e	[7]					
[SS] Servicios subcontratados						
[023] [ADSL] Conexión a internet brindada por un ISP	[9]					
[L] Instalaciones						
[022] [oficina] CELUTEL SAS SINCELEJO CENTRO	[9]					
[P] Personal						
[024] [IS] ingeniero de sistemas	[9]	[9]	[9]	[9]	[9]	
[025] [USER_OP_CONT] contador	[5]	[7]		[8]		
[026] [USER_OP_BOD] administrador bodega	[5]	[7]		[8]		
[027] [USER_OP_CAJA] cajero	[5]	[7]		[8]		

6.5 IDENTIFICACIÓN DE LAS AMENAZAS SEGÚN MAGERIT

Las amenazas son consideradas como todas las posibles situaciones que pueden ocasionar problemas de seguridad, las amenazas se clasifican en cuatro grupos como son: Desastres naturales, de origen industrial, errores y fallos no intencionados y ataques intencionados.[8]

Para llevar a cabo la valoración de las amenazas se utiliza el siguiente escalafón de ocurrencia de tales amenazas

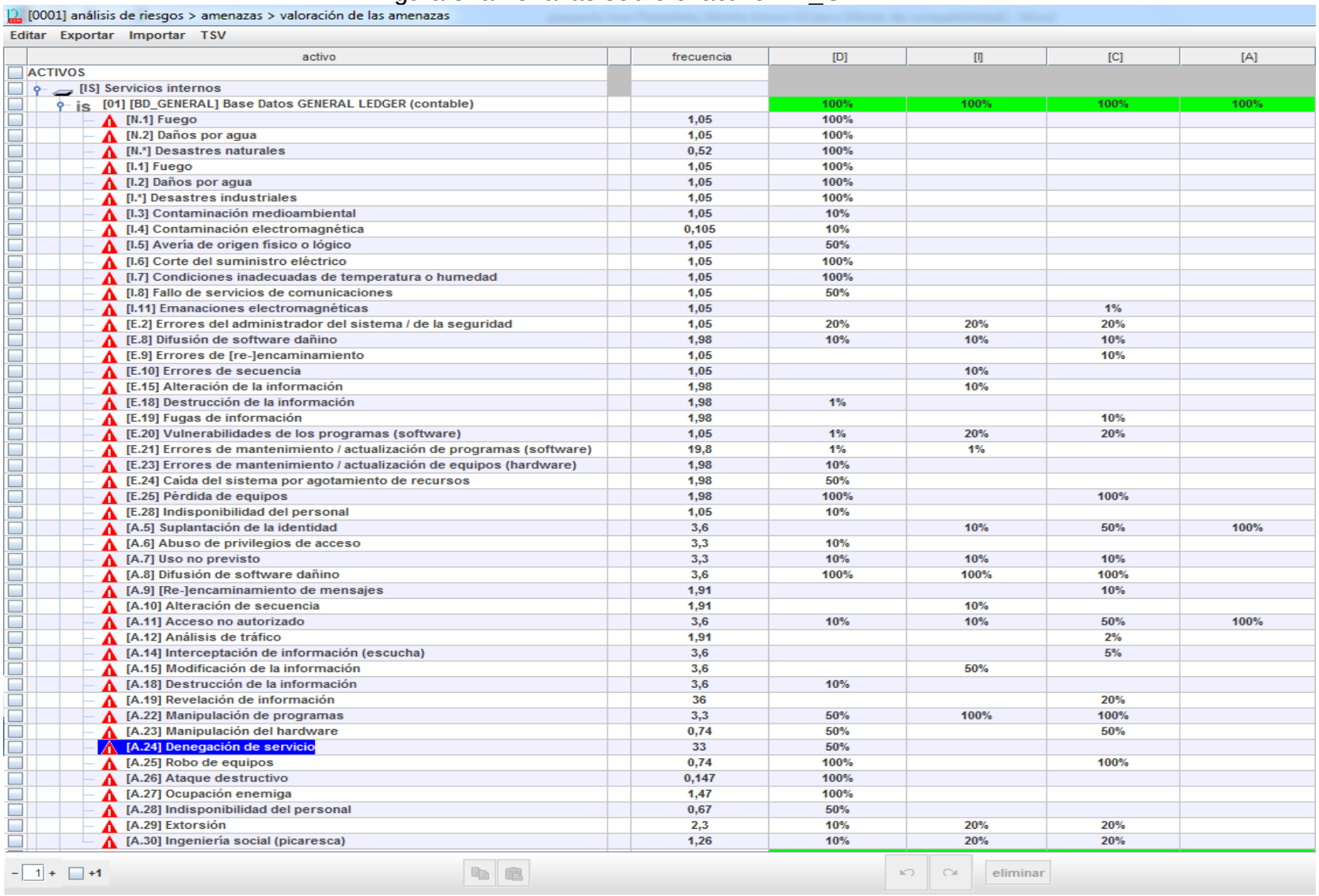
Tabla 6. Probabilidad de ocurrencia de una amenaza según ear/pilar

POTENCIAL	PROBABILIDAD	NIVEL	FACILIDAD	FRECUENCIA
XL extra grande	CS casi seguro	MA muy alto	F fácil	100
L grande	MA muy alta	A Alto	M medio	10
M medio	P posible	M medio	D difícil	1
S pequeño	PP poco probable	B bajo	MD muy difícil	0,1
XS muy pequeño	MR muy rara	MB muy bajo	ED extremadamente difícil	0.01

En las siguientes imágenes se relacionan los activos, las amenazas, y el porcentaje de degradación de cada una de las dimensiones a los cuales afectara en caso de materializarse, para este proceso se utilizó ear/pilar

[8] PORTAL DE ADMINISTRACIÓN ELECTRÓNICA. Magerit V.3: Metodología de análisis y gestión de riesgos de los sistemas de información. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VfhKvvl_Oko

Figura 3: amenazas sobre el activo BD_GENERAL



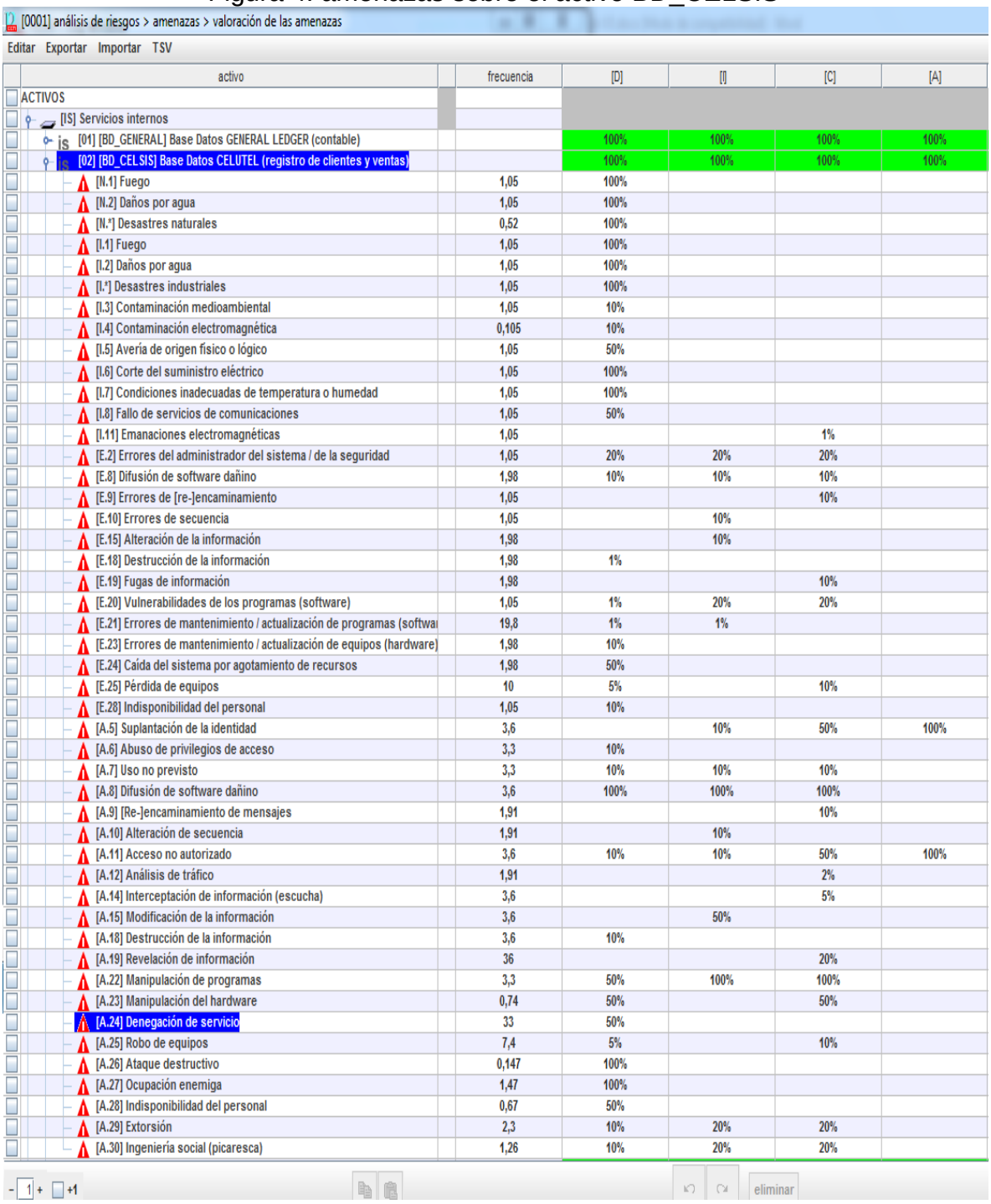
[0001] análisis de riesgos > amenazas > valoración de las amenazas

Editar Exportar Importar TSV

activo	frecuencia	[D]	[I]	[C]	[A]
ACTIVOS					
[IS] Servicios internos					
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)		100%	100%	100%	100%
[N.1] Fuego	1,05	100%			
[N.2] Daños por agua	1,05	100%			
[N.*] Desastres naturales	0,52	100%			
[I.1] Fuego	1,05	100%			
[I.2] Daños por agua	1,05	100%			
[I.*] Desastres industriales	1,05	100%			
[I.3] Contaminación medioambiental	1,05	10%			
[I.4] Contaminación electromagnética	0,105	10%			
[I.5] Avería de origen físico o lógico	1,05	50%			
[I.6] Corte del suministro eléctrico	1,05	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1,05	100%			
[I.8] Fallo de servicios de comunicaciones	1,05	50%			
[I.11] Emanaciones electromagnéticas	1,05			1%	
[E.2] Errores del administrador del sistema / de la seguridad	1,05	20%	20%	20%	
[E.8] Difusión de software dañino	1,98	10%	10%	10%	
[E.9] Errores de [re-]encaminamiento	1,05			10%	
[E.10] Errores de secuencia	1,05		10%		
[E.15] Alteración de la información	1,98		10%		
[E.18] Destrucción de la información	1,98	1%			
[E.19] Fugas de información	1,98			10%	
[E.20] Vulnerabilidades de los programas (software)	1,05	1%	20%	20%	
[E.21] Errores de mantenimiento / actualización de programas (software)	19,8	1%	1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1,98	10%			
[E.24] Caída del sistema por agotamiento de recursos	1,98	50%			
[E.25] Pérdida de equipos	1,98	100%		100%	
[E.28] Indisponibilidad del personal	1,05	10%			
[A.5] Suplantación de la identidad	3,6		10%	50%	100%
[A.6] Abuso de privilegios de acceso	3,3	10%			
[A.7] Uso no previsto	3,3	10%	10%	10%	
[A.8] Difusión de software dañino	3,6	100%	100%	100%	
[A.9] [Re-]encaminamiento de mensajes	1,91			10%	
[A.10] Alteración de secuencia	1,91		10%		
[A.11] Acceso no autorizado	3,6	10%	10%	50%	100%
[A.12] Análisis de tráfico	1,91			2%	
[A.14] Interceptación de información (escucha)	3,6			5%	
[A.15] Modificación de la información	3,6		50%		
[A.18] Destrucción de la información	3,6	10%			
[A.19] Revelación de información	36			20%	
[A.22] Manipulación de programas	3,3	50%	100%	100%	
[A.23] Manipulación del hardware	0,74	50%		50%	
[A.24] Denegación de servicio	33	50%			
[A.25] Robo de equipos	0,74	100%		100%	
[A.26] Ataque destructivo	0,147	100%			
[A.27] Ocupación enemiga	1,47	100%			
[A.28] Indisponibilidad del personal	0,67	50%			
[A.29] Extorsión	2,3	10%	20%	20%	
[A.30] Ingeniería social (picaresca)	1,26	10%	20%	20%	

- 1 + +1 eliminar

Figura 4: amenazas sobre el activo BD_CELSIS



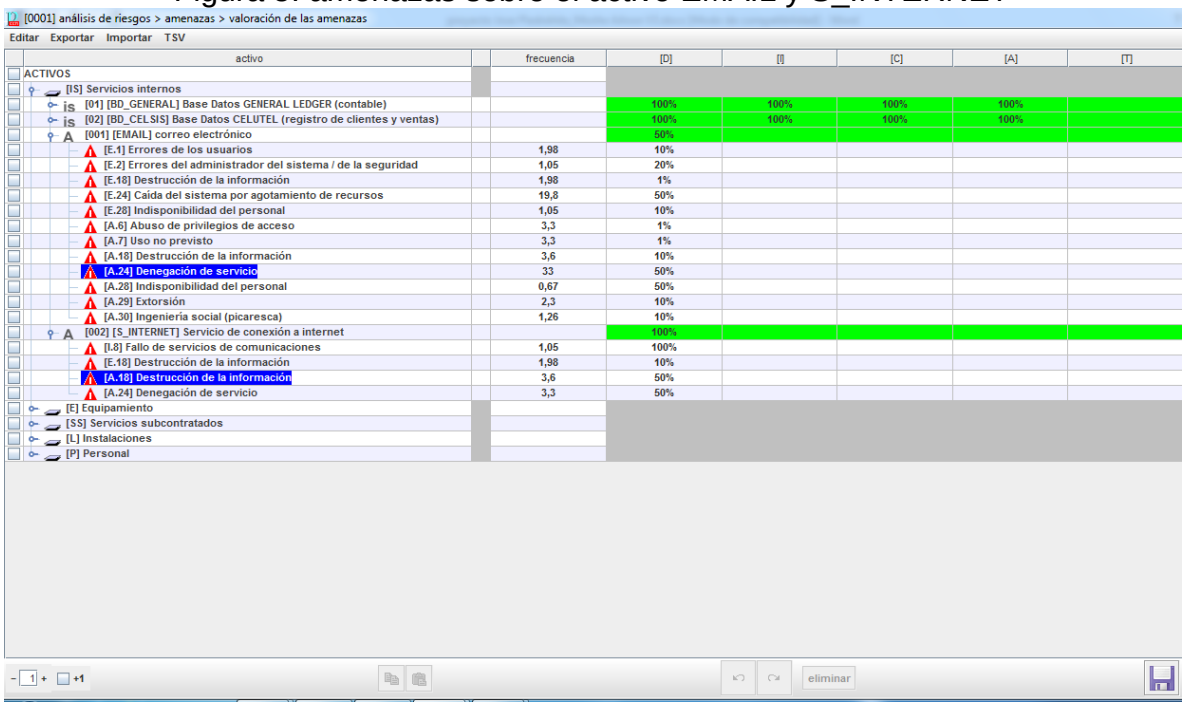
[0001] análisis de riesgos > amenazas > valoración de las amenazas

Editar Exportar Importar TSV

activo	frecuencia	[D]	[I]	[C]	[A]
ACTIVOS					
[IS] Servicios internos					
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)		100%	100%	100%	100%
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)		100%	100%	100%	100%
[N.1] Fuego	1,05	100%			
[N.2] Daños por agua	1,05	100%			
[N.*] Desastres naturales	0,52	100%			
[I.1] Fuego	1,05	100%			
[I.2] Daños por agua	1,05	100%			
[I.*] Desastres industriales	1,05	100%			
[I.3] Contaminación medioambiental	1,05	10%			
[I.4] Contaminación electromagnética	0,105	10%			
[I.5] Avería de origen físico o lógico	1,05	50%			
[I.6] Corte del suministro eléctrico	1,05	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1,05	100%			
[I.8] Fallo de servicios de comunicaciones	1,05	50%			
[I.11] Emanaciones electromagnéticas	1,05			1%	
[E.2] Errores del administrador del sistema / de la seguridad	1,05	20%	20%	20%	
[E.8] Difusión de software dañino	1,98	10%	10%	10%	
[E.9] Errores de [re-]encaminamiento	1,05			10%	
[E.10] Errores de secuencia	1,05		10%		
[E.15] Alteración de la información	1,98		10%		
[E.18] Destrucción de la información	1,98	1%			
[E.19] Fugas de información	1,98			10%	
[E.20] Vulnerabilidades de los programas (software)	1,05	1%	20%	20%	
[E.21] Errores de mantenimiento / actualización de programas (softwa	19,8	1%	1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1,98	10%			
[E.24] Caída del sistema por agotamiento de recursos	1,98	50%			
[E.25] Pérdida de equipos	10	5%		10%	
[E.28] Indisponibilidad del personal	1,05	10%			
[A.5] Suplantación de la identidad	3,6		10%	50%	100%
[A.6] Abuso de privilegios de acceso	3,3	10%			
[A.7] Uso no previsto	3,3	10%	10%	10%	
[A.8] Difusión de software dañino	3,6	100%	100%	100%	
[A.9] [Re-]encaminamiento de mensajes	1,91			10%	
[A.10] Alteración de secuencia	1,91		10%		
[A.11] Acceso no autorizado	3,6	10%	10%	50%	100%
[A.12] Análisis de tráfico	1,91			2%	
[A.14] Interceptación de información (escucha)	3,6			5%	
[A.15] Modificación de la información	3,6		50%		
[A.18] Destrucción de la información	3,6	10%			
[A.19] Revelación de información	36			20%	
[A.22] Manipulación de programas	3,3	50%	100%	100%	
[A.23] Manipulación del hardware	0,74	50%		50%	
[A.24] Denegación de servicio	33	50%			
[A.25] Robo de equipos	7,4	5%		10%	
[A.26] Ataque destructivo	0,147	100%			
[A.27] Ocupación enemiga	1,47	100%			
[A.28] Indisponibilidad del personal	0,67	50%			
[A.29] Extorsión	2,3	10%	20%	20%	
[A.30] Ingeniería social (picaresca)	1,26	10%	20%	20%	

- 1 + +1 eliminar

Figura 5: amenazas sobre el activo EMAIL y S_INTERNET



activo	frecuencia	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
[IS] Servicios internos						
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)		100%	100%	100%	100%	
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)		100%	100%	100%	100%	
[001] [EMAIL] correo electrónico		50%				
[E.1] Errores de los usuarios	1,98	10%				
[E.2] Errores del administrador del sistema / de la seguridad	1,05	20%				
[E.18] Destrucción de la información	1,98	1%				
[E.24] Caida del sistema por agotamiento de recursos	19,8	50%				
[E.28] Indisponibilidad del personal	1,05	10%				
[A.6] Abuso de privilegios de acceso	3,3	1%				
[A.7] Uso no previsto	3,3	1%				
[A.18] Destrucción de la información	3,6	10%				
[A.24] Denegación de servicio	33	50%				
[A.28] Indisponibilidad del personal	0,67	50%				
[A.29] Extorsión	2,3	10%				
[A.30] Ingeniería social (picaresca)	1,26	10%				
[002] [S_INTERNET] Servicio de conexión a internet		100%				
[I.8] Fallo de servicios de comunicaciones	1,05	100%				
[E.18] Destrucción de la información	1,98	10%				
[A.18] Destrucción de la información	3,6	50%				
[A.24] Denegación de servicio	3,3	50%				
[E] Equipamiento						
[SS] Servicios subcontratados						
[L] Instalaciones						
[P] Personal						

Figura 6: amenazas sobre el activo SW_GENERAL LEDGER

activo	frecuencia	[D]	[I]	[C]	[A]
ervicios internos					
uipamiento					
W] Aplicaciones					
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera		100%	100%	100%	
[N.1] Fuego	0,105	100%			
[N.2] Daños por agua	0,105	50%			
[N.*] Desastres naturales	0,105	100%			
[I.1] Fuego	0,52	100%			
[I.2] Daños por agua	0,52	50%			
[I.*] Desastres industriales	0,52	100%			
[I.3] Contaminación medioambiental	0,105	50%			
[I.4] Contaminación electromagnética	1,05	10%			
[I.5] Avería de origen físico o lógico	1,05	50%			
[I.6] Corte del suministro eléctrico	1,05	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1,05	100%			
[I.11] Emanaciones electromagnéticas	1,05			1%	
[E.8] Difusión de software dañino	1,98	10%	10%	10%	
[E.20] Vulnerabilidades de los programas (software)	1,05	1%	20%	20%	
[E.21] Errores de mantenimiento / actualización de programas (software)	19,8	1%	1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1,98	10%			
[E.24] Caida del sistema por agotamiento de recursos	19,8	50%			
[E.25] Pérdida de equipos	1,98	100%		100%	
[A.7] Uso no previsto	3,3	1%	1%	10%	
[A.8] Difusión de software dañino	3,6	100%	100%	100%	
[A.11] Acceso no autorizado	3,6	10%	10%	50%	
[A.22] Manipulación de programas	3,3	50%	100%	100%	
[A.23] Manipulación del hardware	0,74	50%		50%	
[A.24] Denegación de servicio	6,6	100%			
[A.25] Robo de equipos	0,74	100%		100%	
[A.26] Ataque destructivo	1,47	100%			

Figura 7: amenazas sobre el activo PL_POLIEDRO

activo	frecuencia	[D]	[I]	[C]	[A]
Servicios internos					
:quipamiento					
SW] Aplicaciones					
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera		100%	100%	100%	
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y pl		100%	100%	100%	100%
[I.5] Avería de origen físico o lógico	1,05	50%			
[I.8] Fallo de servicios de comunicaciones	1,05	50%			
[E.2] Errores del administrador del sistema / de la seguridad	1,05	20%	20%	20%	
[E.8] Difusión de software dañino	1,98	10%	10%	10%	
[E.9] Errores de [re-]encaminamiento	1,05			10%	
[E.10] Errores de secuencia	1,05		10%		
[E.15] Alteración de la información	1,98		1%		
[E.19] Fugas de información	1,98			10%	
[E.20] Vulnerabilidades de los programas (software)	1,05	1%	20%	20%	
[E.21] Errores de mantenimiento / actualización de programas (software)	19,8	1%	1%		
[E.24] Caída del sistema por agotamiento de recursos	1,98	50%			
[A.5] Suplantación de la identidad	3,6		10%	50%	100%
[A.7] Uso no previsto	3,3	10%	10%	10%	
[A.8] Difusión de software dañino	3,6	100%	100%	100%	
[A.9] [Re-]encaminamiento de mensajes	1,91			10%	
[A.10] Alteración de secuencia	1,91		10%		
[A.11] Acceso no autorizado	3,6		10%	50%	100%
[A.12] Análisis de tráfico	1,91			2%	
[A.14] Interceptación de información (escucha)	3,6			5%	
[A.15] Modificación de la información	3,6		10%		
[A.18] Destrucción de la información	3,6	50%			
[A.22] Manipulación de programas	3,3	50%	100%	100%	
[A.24] Denegación de servicio	33	50%			

Figura 8: amenazas sobre el activo SW_CELSIS

activo	frecuencia	[D]	[I]	[C]
Servicios internos				
Equipamiento				
[SW] Aplicaciones				
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera		100%	100%	100%
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y pl		100%	100%	100%
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas		100%	100%	100%
[N.1] Fuego	0,105	100%		
[N.2] Daños por agua	0,105	50%		
[N.*] Desastres naturales	0,105	100%		
[I.1] Fuego	0,52	100%		
[I.2] Daños por agua	0,52	50%		
[I.*] Desastres industriales	0,52	100%		
[I.3] Contaminación medioambiental	0,105	50%		
[I.4] Contaminación electromagnética	1,05	10%		
[I.5] Avería de origen físico o lógico	1,05	50%		
[I.6] Corte del suministro eléctrico	1,05	100%		
[I.7] Condiciones inadecuadas de temperatura o humedad	1,05	100%		
[I.11] Emanaciones electromagnéticas	1,05			1%
[E.8] Difusión de software dañino	1,98	10%	10%	10%
[E.20] Vulnerabilidades de los programas (software)	1,05	1%	20%	20%
[E.21] Errores de mantenimiento / actualización de programas (software)	19,8	1%	1%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1,98	10%		
[E.24] Caída del sistema por agotamiento de recursos	19,8	50%		
[E.25] Pérdida de equipos	1,98	100%		100%
[A.7] Uso no previsto	3,3	1%	1%	10%
[A.8] Difusión de software dañino	3,6	100%	100%	100%
[A.11] Acceso no autorizado	3,6	10%	10%	50%
[A.22] Manipulación de programas	3,3	50%	100%	100%
[A.23] Manipulación del hardware	0,74	50%		50%
[A.24] Denegación de servicio	6,6	100%		
[A.25] Robo de equipos	0,74	100%		100%
[A.26] Ataque destructivo	1,47	100%		

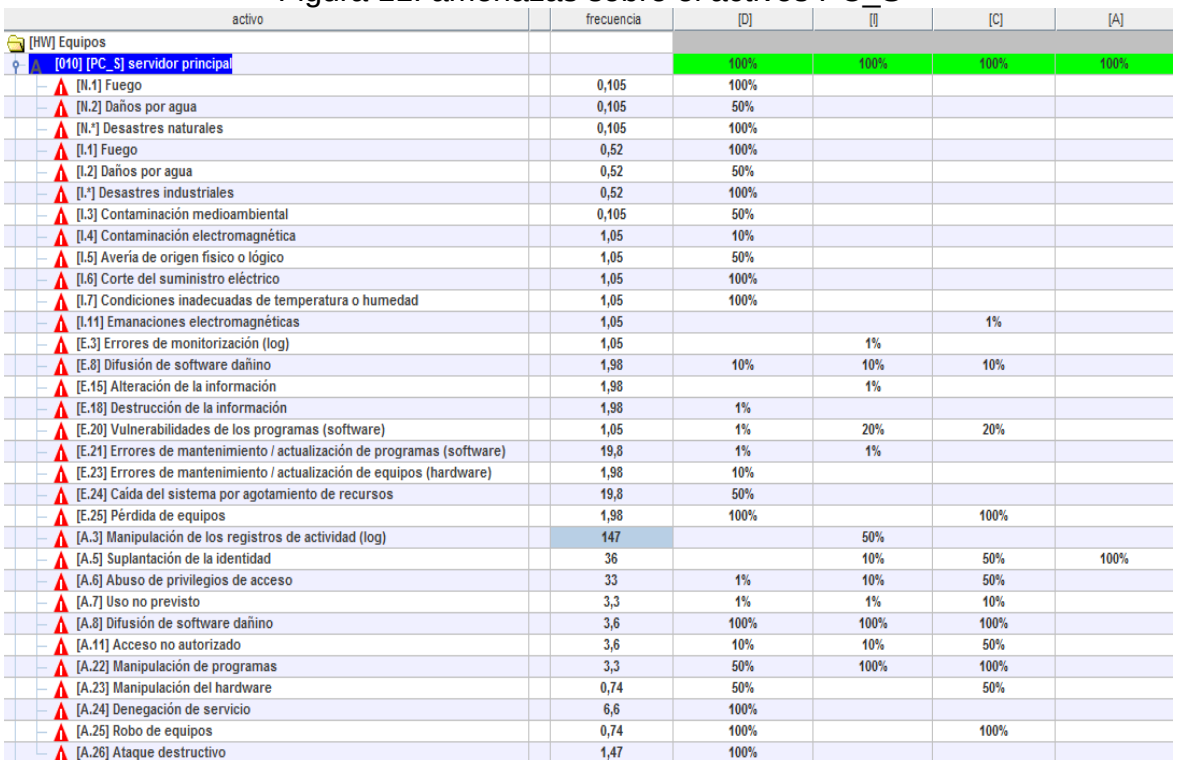
Figura 9: amenazas sobre el activo SQL_SERVER

activo	frecuencia	[D]	[I]	[C]	[A]
[SW] Aplicaciones					
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera		100%	100%	100%	
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y pl		100%	100%	100%	100%
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas		100%	100%	100%	
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales		100%	100%	100%	
[N.1] Fuego	0,105	100%			
[N.2] Daños por agua	0,105	50%			
[N.*] Desastres naturales	0,105	100%			
[I.1] Fuego	0,52	100%			
[I.2] Daños por agua	0,52	50%			
[I.*] Desastres industriales	0,52	100%			
[I.3] Contaminación medioambiental	0,105	50%			
[I.4] Contaminación electromagnética	1,05	10%			
[I.5] Avería de origen físico o lógico	1,05	50%			
[I.6] Corte del suministro eléctrico	1,05	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1,05	100%			
[I.11] Emanaciones electromagnéticas	1,05			1%	
[E.8] Difusión de software dañino	1,98	10%	10%	10%	
[E.20] Vulnerabilidades de los programas (software)	1,05	1%	20%	20%	
[E.21] Errores de mantenimiento / actualización de programas (software)	19,8	1%	1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1,98	10%			
[E.24] Caída del sistema por agotamiento de recursos	19,8	50%			
[E.25] Pérdida de equipos	1,98	100%		100%	
[A.7] Uso no previsto	3,3	1%	1%	10%	
[A.8] Difusión de software dañino	3,6	100%	100%	100%	
[A.11] Acceso no autorizado	3,6	10%	10%	50%	
[A.22] Manipulación de programas	3,3	50%	100%	100%	
[A.23] Manipulación del hardware	0,74	50%		50%	
[A.24] Denegación de servicio	6,6	100%			
[A.25] Robo de equipos	0,74	100%		100%	
[A.26] Ataque destructivo	1,47	100%			

Figura 10: amenazas sobre el activos SO, OFFICE y AV

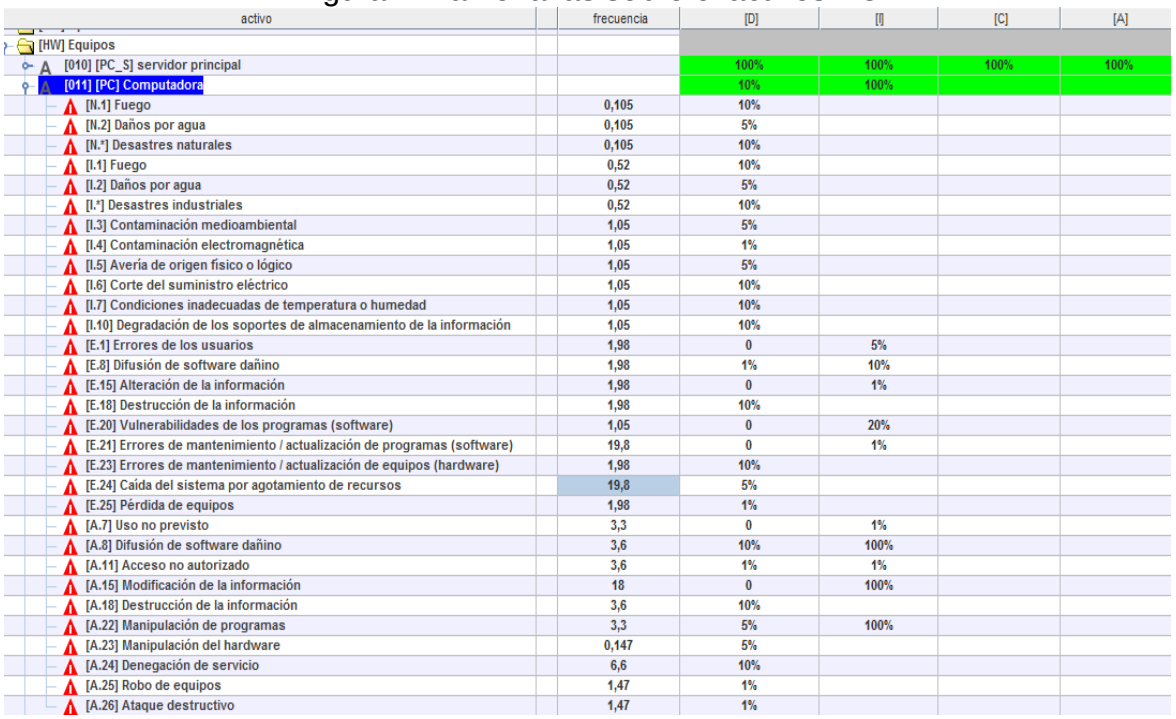
activo	frecuencia	[D]	[I]	[C]	[A]
S					
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera		100%	100%	100%	
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y pla		100%	100%	100%	100%
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas		100%	100%	100%	
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales		100%	100%	100%	
[007] [SO] Sistema Operativo		100%	100%	100%	
[I.5] Avería de origen físico o lógico	1,05	50%			
[E.8] Difusión de software dañino	1,98	10%	10%	10%	
[E.20] Vulnerabilidades de los programas (software)	1,05	1%	20%	20%	
[E.21] Errores de mantenimiento / actualización de programas (software)	19,8	1%	1%		
[A.8] Difusión de software dañino	3,6	100%	100%	100%	
[A.22] Manipulación de programas	3,3	50%	100%	100%	
[008] [OFFICE] ofimática		100%	100%		
[I.5] Avería de origen físico o lógico	1,05	50%			
[E.8] Difusión de software dañino	1,98	10%	10%		
[E.20] Vulnerabilidades de los programas (software)	1,05	1%	20%		
[E.21] Errores de mantenimiento / actualización de programas (software)	19,8	1%	1%		
[A.8] Difusión de software dañino	3,6	100%	100%		
[A.22] Manipulación de programas	3,3	50%	100%		
[009] [AV] Anti virus		100%	100%	100%	
[I.5] Avería de origen físico o lógico	1,05	50%			
[E.8] Difusión de software dañino	1,98	10%	10%	10%	
[E.20] Vulnerabilidades de los programas (software)	1,05	1%	20%	20%	
[E.21] Errores de mantenimiento / actualización de programas (software)	19,8	1%	1%		
[A.8] Difusión de software dañino	3,6	100%	100%	100%	
[A.22] Manipulación de programas	3,3	50%	100%	100%	

Figura 11: amenazas sobre el activos PC_S



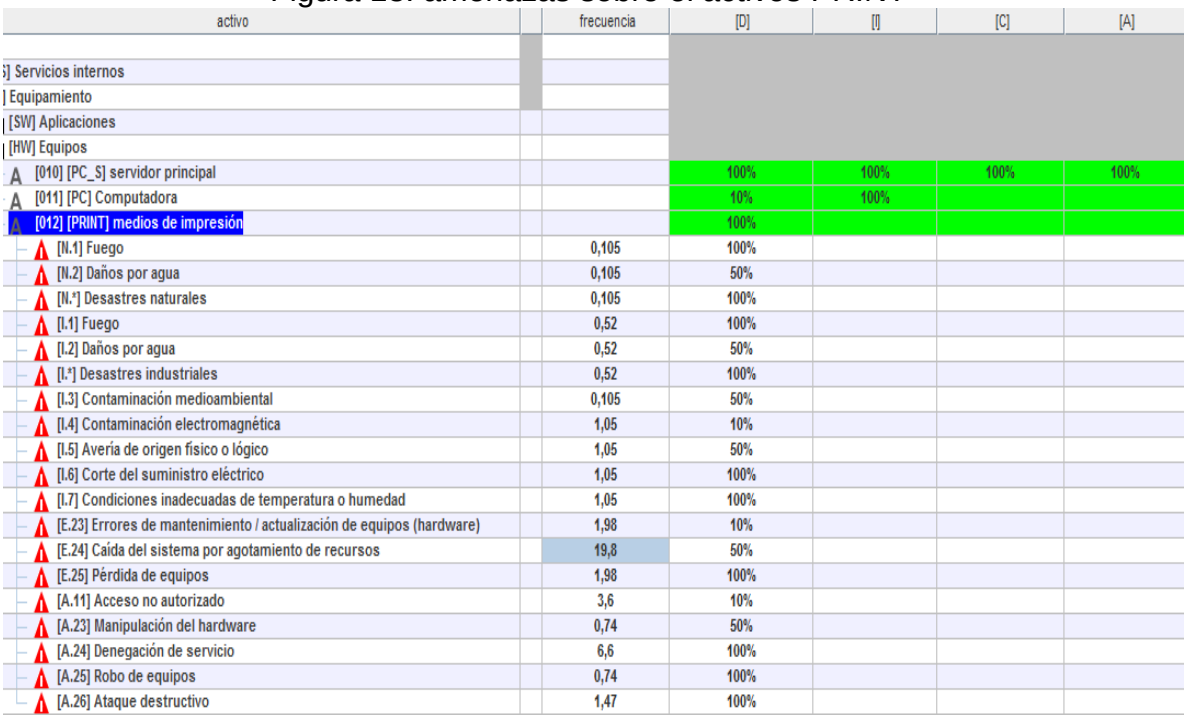
activo	frecuencia	[D]	[I]	[C]	[A]
[HW] Equipos					
[010] [PC_S] servidor principal		100%	100%	100%	100%
[N.1] Fuego	0,105	100%			
[N.2] Daños por agua	0,105	50%			
[N.*] Desastres naturales	0,105	100%			
[I.1] Fuego	0,52	100%			
[I.2] Daños por agua	0,52	50%			
[I.*] Desastres industriales	0,52	100%			
[I.3] Contaminación medioambiental	0,105	50%			
[I.4] Contaminación electromagnética	1,05	10%			
[I.5] Avería de origen físico o lógico	1,05	50%			
[I.6] Corte del suministro eléctrico	1,05	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1,05	100%			
[I.11] Emanaciones electromagnéticas	1,05			1%	
[E.3] Errores de monitorización (log)	1,05		1%		
[E.8] Difusión de software dañino	1,98	10%	10%	10%	
[E.15] Alteración de la información	1,98		1%		
[E.18] Destrucción de la información	1,98	1%			
[E.20] Vulnerabilidades de los programas (software)	1,05	1%	20%	20%	
[E.21] Errores de mantenimiento / actualización de programas (software)	19,8	1%	1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1,98	10%			
[E.24] Caída del sistema por agotamiento de recursos	19,8	50%			
[E.25] Pérdida de equipos	1,98	100%		100%	
[A.3] Manipulación de los registros de actividad (log)	147		50%		
[A.5] Suplantación de la identidad	36		10%	50%	100%
[A.6] Abuso de privilegios de acceso	33	1%	10%	50%	
[A.7] Uso no previsto	3,3	1%	1%	10%	
[A.8] Difusión de software dañino	3,6	100%	100%	100%	
[A.11] Acceso no autorizado	3,6	10%	10%	50%	
[A.22] Manipulación de programas	3,3	50%	100%	100%	
[A.23] Manipulación del hardware	0,74	50%		50%	
[A.24] Denegación de servicio	6,6	100%			
[A.25] Robo de equipos	0,74	100%		100%	
[A.26] Ataque destructivo	1,47	100%			

Figura 12: amenazas sobre el activos PC



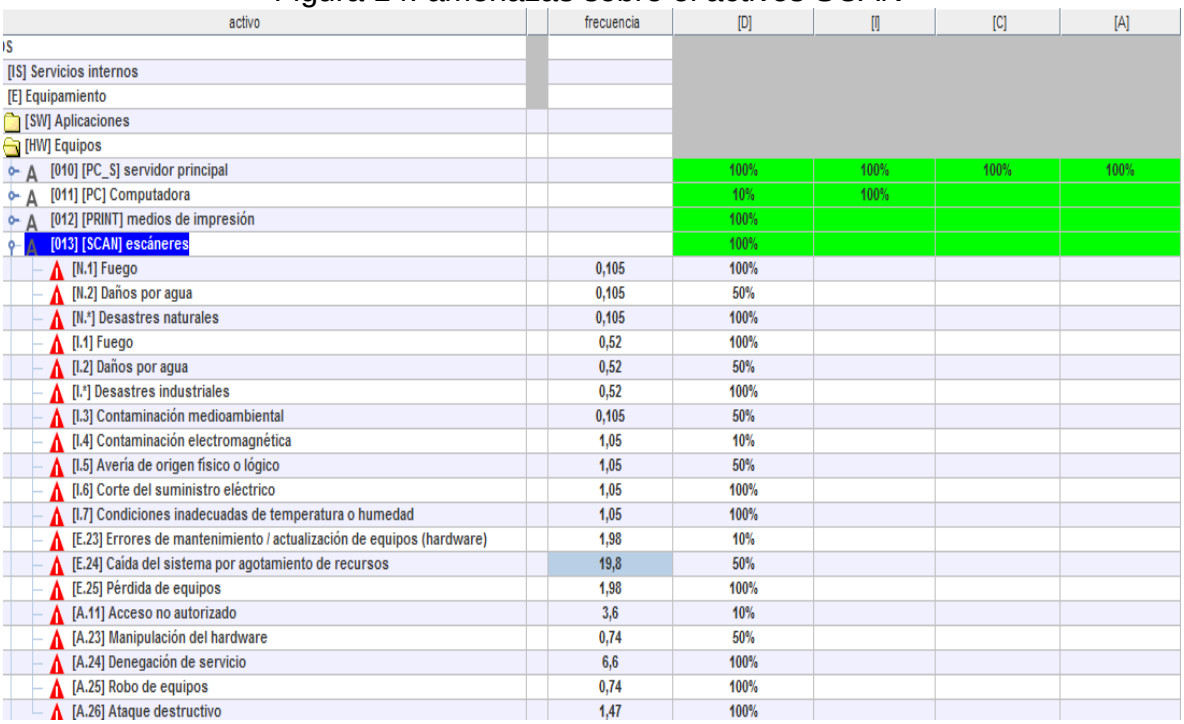
activo	frecuencia	[D]	[I]	[C]	[A]
[HW] Equipos					
[010] [PC_S] servidor principal		100%	100%	100%	100%
[011] [PC] Computadora		10%	100%		
[N.1] Fuego	0,105	10%			
[N.2] Daños por agua	0,105	5%			
[N.*] Desastres naturales	0,105	10%			
[I.1] Fuego	0,52	10%			
[I.2] Daños por agua	0,52	5%			
[I.*] Desastres industriales	0,52	10%			
[I.3] Contaminación medioambiental	1,05	5%			
[I.4] Contaminación electromagnética	1,05	1%			
[I.5] Avería de origen físico o lógico	1,05	5%			
[I.6] Corte del suministro eléctrico	1,05	10%			
[I.7] Condiciones inadecuadas de temperatura o humedad	1,05	10%			
[I.10] Degradación de los soportes de almacenamiento de la información	1,05	10%			
[E.1] Errores de los usuarios	1,98	0	5%		
[E.8] Difusión de software dañino	1,98	1%	10%		
[E.15] Alteración de la información	1,98	0	1%		
[E.18] Destrucción de la información	1,98	10%			
[E.20] Vulnerabilidades de los programas (software)	1,05	0	20%		
[E.21] Errores de mantenimiento / actualización de programas (software)	19,8	0	1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1,98	10%			
[E.24] Caída del sistema por agotamiento de recursos	19,8	5%			
[E.25] Pérdida de equipos	1,98	1%			
[A.7] Uso no previsto	3,3	0	1%		
[A.8] Difusión de software dañino	3,6	10%	100%		
[A.11] Acceso no autorizado	3,6	1%	1%		
[A.15] Modificación de la información	18	0	100%		
[A.18] Destrucción de la información	3,6	10%			
[A.22] Manipulación de programas	3,3	5%	100%		
[A.23] Manipulación del hardware	0,147	5%			
[A.24] Denegación de servicio	6,6	10%			
[A.25] Robo de equipos	1,47	1%			
[A.26] Ataque destructivo	1,47	1%			

Figura 13: amenazas sobre el activos PRINT



activo		frecuencia	[D]	[I]	[C]	[A]
] Servicios internos						
] Equipamiento						
[SW] Aplicaciones						
[HW] Equipos						
[010] [PC_S] servidor principal			100%	100%	100%	100%
[011] [PC] Computadora			10%	100%		
[012] [PRINT] medios de impresión			100%			
[N.1] Fuego		0,105	100%			
[N.2] Daños por agua		0,105	50%			
[N.*] Desastres naturales		0,105	100%			
[I.1] Fuego		0,52	100%			
[I.2] Daños por agua		0,52	50%			
[I.*] Desastres industriales		0,52	100%			
[I.3] Contaminación medioambiental		0,105	50%			
[I.4] Contaminación electromagnética		1,05	10%			
[I.5] Avería de origen físico o lógico		1,05	50%			
[I.6] Corte del suministro eléctrico		1,05	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad		1,05	100%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1,98	10%			
[E.24] Caída del sistema por agotamiento de recursos		19,8	50%			
[E.25] Pérdida de equipos		1,98	100%			
[A.11] Acceso no autorizado		3,6	10%			
[A.23] Manipulación del hardware		0,74	50%			
[A.24] Denegación de servicio		6,6	100%			
[A.25] Robo de equipos		0,74	100%			
[A.26] Ataque destructivo		1,47	100%			

Figura 14: amenazas sobre el activos SCAN



activo		frecuencia	[D]	[I]	[C]	[A]
S						
[S] Servicios internos						
[E] Equipamiento						
[SW] Aplicaciones						
[HW] Equipos						
[010] [PC_S] servidor principal			100%	100%	100%	100%
[011] [PC] Computadora			10%	100%		
[012] [PRINT] medios de impresión			100%			
[013] [SCAN] escáneres			100%			
[N.1] Fuego		0,105	100%			
[N.2] Daños por agua		0,105	50%			
[N.*] Desastres naturales		0,105	100%			
[I.1] Fuego		0,52	100%			
[I.2] Daños por agua		0,52	50%			
[I.*] Desastres industriales		0,52	100%			
[I.3] Contaminación medioambiental		0,105	50%			
[I.4] Contaminación electromagnética		1,05	10%			
[I.5] Avería de origen físico o lógico		1,05	50%			
[I.6] Corte del suministro eléctrico		1,05	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad		1,05	100%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1,98	10%			
[E.24] Caída del sistema por agotamiento de recursos		19,8	50%			
[E.25] Pérdida de equipos		1,98	100%			
[A.11] Acceso no autorizado		3,6	10%			
[A.23] Manipulación del hardware		0,74	50%			
[A.24] Denegación de servicio		6,6	100%			
[A.25] Robo de equipos		0,74	100%			
[A.26] Ataque destructivo		1,47	100%			

Figura 15: amenazas sobre el activos SWITCH

activo		frecuencia	[D]	[I]	[C]	[A]
S						
[IS] Servicios internos						
[E] Equipamiento						
[SW] Aplicaciones						
[HW] Equipos						
[010] [PC_S] servidor principal			100%	100%	100%	100%
[011] [PC] Computadora			10%	100%		
[012] [PRINT] medios de impresión			100%			
[013] [SCAN] escáneres			100%			
[014] [SWITCH] concentrador red local			100%			
[N.1] Fuego		0,105	100%			
[N.2] Daños por agua		0,105	50%			
[N.*] Desastres naturales		0,105	100%			
[I.1] Fuego		0,52	100%			
[I.2] Daños por agua		0,52	50%			
[I.*] Desastres industriales		0,52	100%			
[I.3] Contaminación medioambiental		0,105	50%			
[I.4] Contaminación electromagnética		1,05	10%			
[I.5] Avería de origen físico o lógico		1,05	50%			
[I.6] Corte del suministro eléctrico		1,05	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad		1,05	100%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1,98	10%			
[E.24] Caída del sistema por agotamiento de recursos		19,8	50%			
[E.25] Pérdida de equipos		1,98	20%			
[A.7] Uso no previsto		3,3	10%			
[A.11] Acceso no autorizado		3,6	10%			
[A.23] Manipulación del hardware		0,74	100%			
[A.24] Denegación de servicio		6,6	100%			
[A.25] Robo de equipos		0,74	20%			
[A.26] Ataque destructivo		1,47	100%			

Figura 16: amenazas sobre el activos CONMUTADOR

activo		frecuencia	[D]	[I]	[C]	[A]
S						
[IS] Servicios internos						
[E] Equipamiento						
[SW] Aplicaciones						
[HW] Equipos						
[010] [PC_S] servidor principal			100%	100%	100%	100%
[011] [PC] Computadora			10%	100%		
[012] [PRINT] medios de impresión			100%			
[013] [SCAN] escáneres			100%			
[014] [SWITCH] concentrador red local			100%			
[015] [CONMUTADOR] conmutador interno telefonico			100%			
[N.1] Fuego		0,105	100%			
[N.2] Daños por agua		0,105	50%			
[N.*] Desastres naturales		0,105	100%			
[I.1] Fuego		0,52	100%			
[I.2] Daños por agua		0,52	50%			
[I.*] Desastres industriales		0,52	100%			
[I.3] Contaminación medioambiental		0,105	50%			
[I.4] Contaminación electromagnética		1,05	10%			
[I.5] Avería de origen físico o lógico		1,05	50%			
[I.6] Corte del suministro eléctrico		1,05	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad		1,05	100%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1,98	10%			
[E.24] Caída del sistema por agotamiento de recursos		19,8	50%			
[E.25] Pérdida de equipos		1,98	100%			
[A.11] Acceso no autorizado		3,6	10%			
[A.23] Manipulación del hardware		0,74	50%			
[A.24] Denegación de servicio		6,6	100%			
[A.25] Robo de equipos		0,74	100%			
[A.26] Ataque destructivo		1,47	100%			

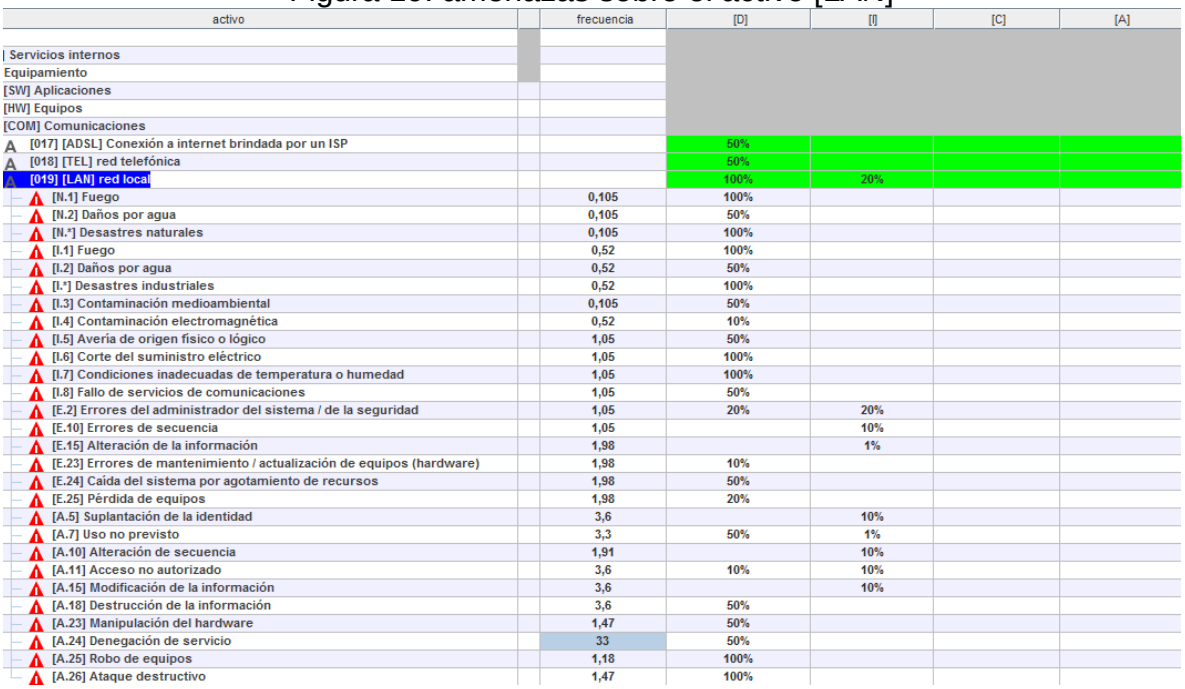
Figura 17: amenazas sobre el activos CAMARA

activo		frecuencia	[D]	[I]	[C]	[A]
[S] Servicios internos						
[E] Equipamiento						
[SW] Aplicaciones						
[HW] Equipos						
[010] [PC_S] servidor principal			100%	100%	100%	100%
[011] [PC] Computadora			10%	100%		
[012] [PRINT] medios de impresión			100%			
[013] [SCAN] escáneres			100%			
[014] [SWITCH] concentrador red local			100%			
[015] [CONMUTADOR] conmutador interno telefonico			100%			
[016] [CÁMARA] cámaras de seguridad			100%			
[N.1] Fuego		0,105	100%			
[N.2] Daños por agua		0,105	50%			
[N.*] Desastres naturales		0,105	100%			
[I.1] Fuego		0,52	100%			
[I.2] Daños por agua		0,52	50%			
[I.*] Desastres industriales		0,52	100%			
[I.3] Contaminación medioambiental		0,105	50%			
[I.4] Contaminación electromagnética		1,05	10%			
[I.5] Avería de origen físico o lógico		1,05	50%			
[I.6] Corte del suministro eléctrico		1,05	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad		1,05	100%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1,98	10%			
[E.24] Caída del sistema por agotamiento de recursos		19,8	50%			
[E.25] Pérdida de equipos		1,98	100%			
[A.11] Acceso no autorizado		3,6	10%			
[A.23] Manipulación del hardware		0,74	50%			
[A.24] Denegación de servicio		6,6	100%			
[A.25] Robo de equipos		0,74	100%			
[A.26] Ataque destructivo		1,47	100%			

Figura 18: amenazas sobre los activos ADSL y TEL

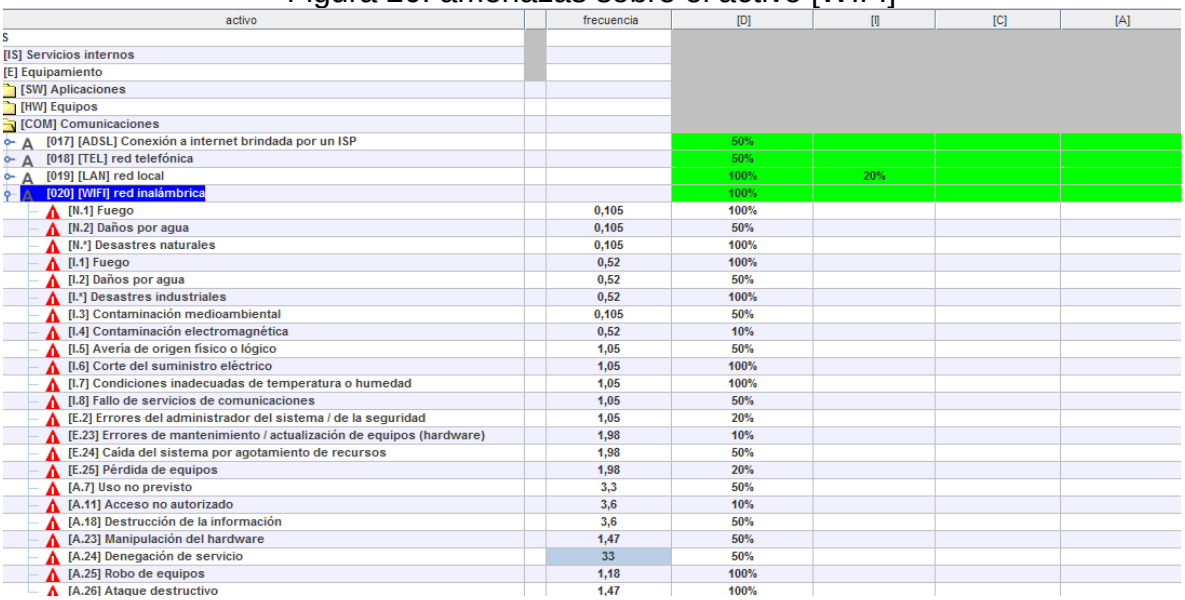
activo		frecuencia	[D]	[I]	[C]	[A]
S						
[IS] Servicios internos						
[E] Equipamiento						
[SW] Aplicaciones						
[HW] Equipos						
[COM] Comunicaciones						
[017] [ADSL] Conexión a internet brindada por un ISP			50%			
[I.8] Fallo de servicios de comunicaciones		1,05	50%			
[E.2] Errores del administrador del sistema / de la seguridad		1,05	20%			
[E.24] Caída del sistema por agotamiento de recursos		1,98	50%			
[A.7] Uso no previsto		3,3	10%			
[A.18] Destrucción de la información		3,6	50%			
[A.24] Denegación de servicio		33	50%			
[018] [TEL] red telefónica			50%			
[I.8] Fallo de servicios de comunicaciones		1,05	50%			
[E.2] Errores del administrador del sistema / de la seguridad		1,05	20%			
[E.24] Caída del sistema por agotamiento de recursos		1,98	50%			
[A.7] Uso no previsto		3,3	10%			
[A.18] Destrucción de la información		3,6	50%			
[A.24] Denegación de servicio		33	50%			

Figura 19: amenazas sobre el activo [LAN]



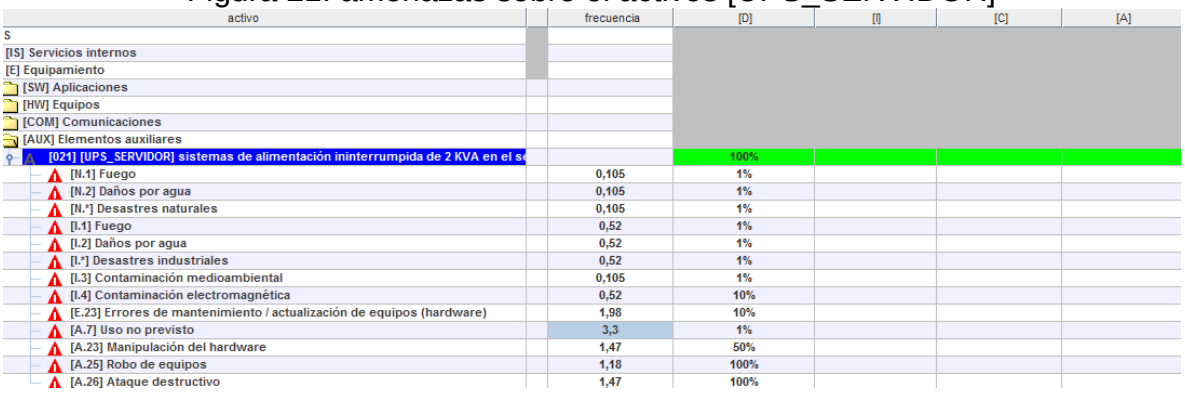
activo		frecuencia	[D]	[I]	[C]	[A]
Servicios internos						
Equipamiento						
[SW] Aplicaciones						
[HW] Equipos						
[COM] Comunicaciones						
[017] [ADSL] Conexión a internet brindada por un ISP			50%			
[018] [TEL] red telefónica			50%			
[019] [LAN] red local			100%	20%		
[N.1] Fuego		0,105	100%			
[N.2] Daños por agua		0,105	50%			
[N.*] Desastres naturales		0,105	100%			
[I.1] Fuego		0,52	100%			
[I.2] Daños por agua		0,52	50%			
[I.*] Desastres industriales		0,52	100%			
[I.3] Contaminación medioambiental		0,105	50%			
[I.4] Contaminación electromagnética		0,52	10%			
[I.5] Avería de origen físico o lógico		1,05	50%			
[I.6] Corte del suministro eléctrico		1,05	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad		1,05	100%			
[I.8] Fallo de servicios de comunicaciones		1,05	50%			
[E.2] Errores del administrador del sistema / de la seguridad		1,05	20%	20%		
[E.10] Errores de secuencia		1,05		10%		
[E.15] Alteración de la información		1,98		1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1,98	10%			
[E.24] Caída del sistema por agotamiento de recursos		1,98	50%			
[E.25] Pérdida de equipos		1,98	20%			
[A.5] Suplantación de la identidad		3,6		10%		
[A.7] Uso no previsto		3,3	50%	1%		
[A.10] Alteración de secuencia		1,91		10%		
[A.11] Acceso no autorizado		3,6	10%	10%		
[A.15] Modificación de la información		3,6		10%		
[A.18] Destrucción de la información		3,6	50%			
[A.23] Manipulación del hardware		1,47	50%			
[A.24] Denegación de servicio		33	50%			
[A.25] Robo de equipos		1,18	100%			
[A.26] Ataque destructivo		1,47	100%			

Figura 20: amenazas sobre el activo [WIFI]



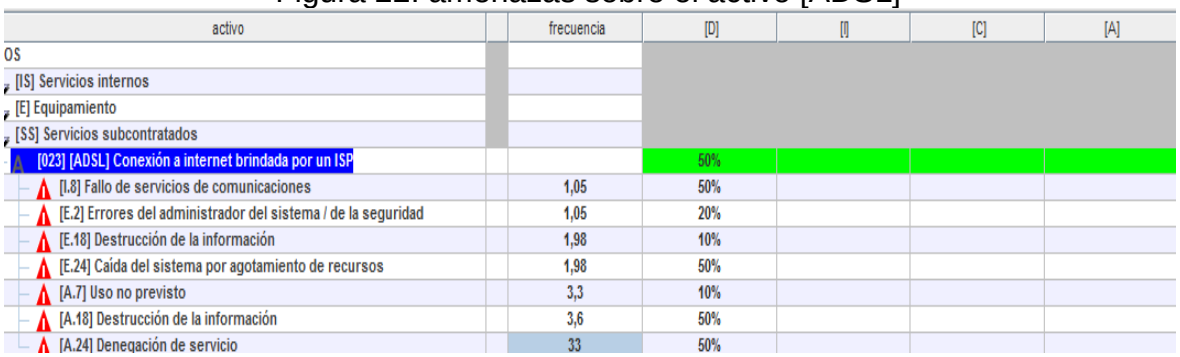
activo		frecuencia	[D]	[I]	[C]	[A]
S						
[IS] Servicios internos						
[E] Equipamiento						
[SW] Aplicaciones						
[HW] Equipos						
[COM] Comunicaciones						
[017] [ADSL] Conexión a internet brindada por un ISP			50%			
[018] [TEL] red telefónica			50%			
[019] [LAN] red local			100%	20%		
[020] [WIFI] red inalámbrica			100%			
[N.1] Fuego		0,105	100%			
[N.2] Daños por agua		0,105	50%			
[N.*] Desastres naturales		0,105	100%			
[I.1] Fuego		0,52	100%			
[I.2] Daños por agua		0,52	50%			
[I.*] Desastres industriales		0,52	100%			
[I.3] Contaminación medioambiental		0,105	50%			
[I.4] Contaminación electromagnética		0,52	10%			
[I.5] Avería de origen físico o lógico		1,05	50%			
[I.6] Corte del suministro eléctrico		1,05	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad		1,05	100%			
[I.8] Fallo de servicios de comunicaciones		1,05	50%			
[E.2] Errores del administrador del sistema / de la seguridad		1,05	20%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1,98	10%			
[E.24] Caída del sistema por agotamiento de recursos		1,98	50%			
[E.25] Pérdida de equipos		1,98	20%			
[A.7] Uso no previsto		3,3	50%			
[A.11] Acceso no autorizado		3,6	10%			
[A.18] Destrucción de la información		3,6	50%			
[A.23] Manipulación del hardware		1,47	50%			
[A.24] Denegación de servicio		33	50%			
[A.25] Robo de equipos		1,18	100%			
[A.26] Ataque destructivo		1,47	100%			

Figura 21: amenazas sobre el activos [UPS_SERVIDOR]



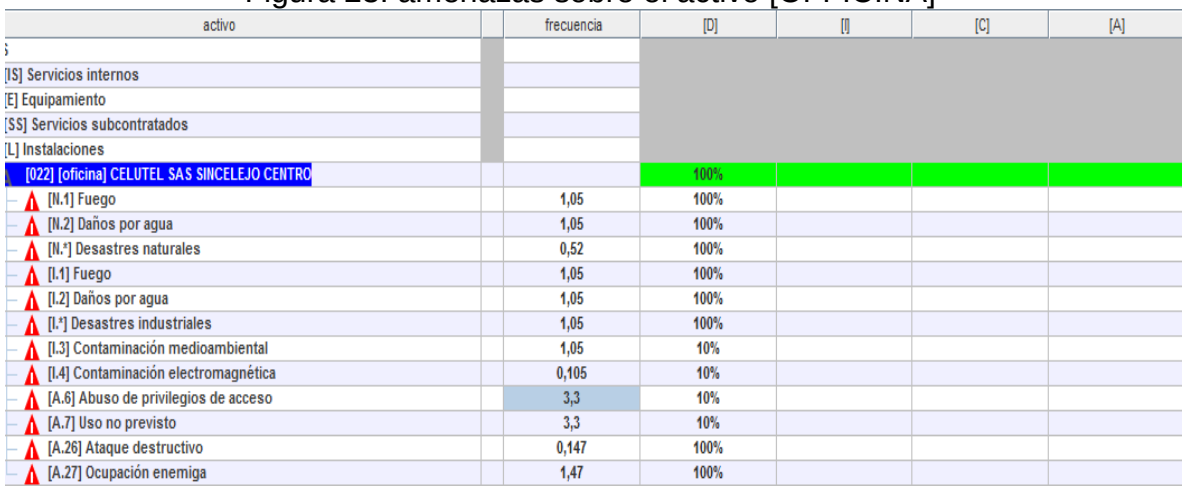
activo		frecuencia	[D]	[I]	[C]	[A]
s						
[IS] Servicios internos						
[E] Equipamiento						
[SW] Aplicaciones						
[HW] Equipos						
[COM] Comunicaciones						
[AUX] Elementos auxiliares						
[021] [UPS_SERVIDOR] sistemas de alimentación ininterrumpida de 2 KVA en el s			100%			
[N.1] Fuego		0,105	1%			
[N.2] Daños por agua		0,105	1%			
[N.*] Desastres naturales		0,105	1%			
[I.1] Fuego		0,52	1%			
[I.2] Daños por agua		0,52	1%			
[I.*] Desastres industriales		0,52	1%			
[I.3] Contaminación medioambiental		0,105	1%			
[I.4] Contaminación electromagnética		0,52	10%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1,98	10%			
[A.7] Uso no previsto		3,3	1%			
[A.23] Manipulación del hardware		1,47	50%			
[A.25] Robo de equipos		1,18	100%			
[A.26] Ataque destructivo		1,47	100%			

Figura 22: amenazas sobre el activo [ADSL]



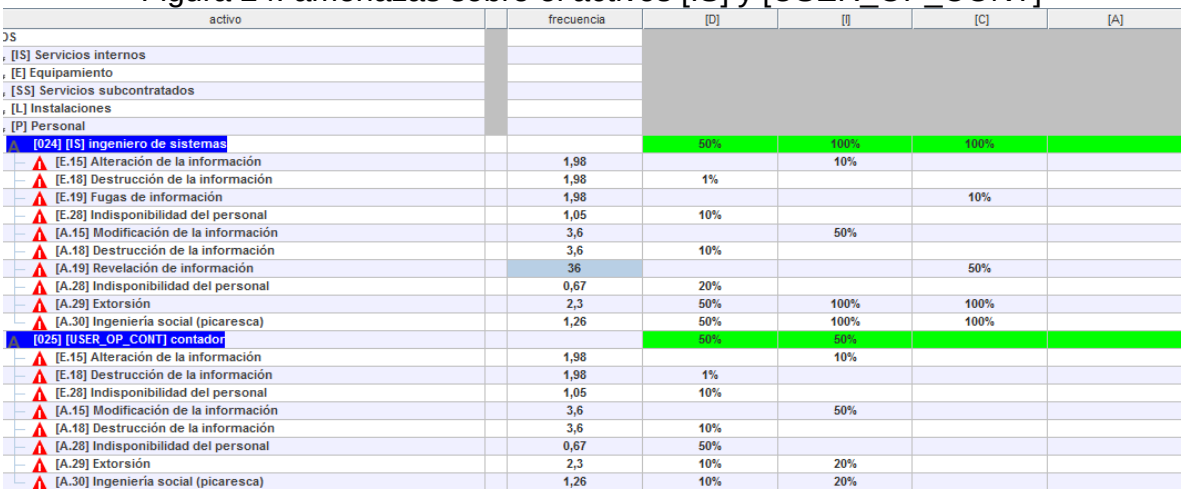
activo		frecuencia	[D]	[I]	[C]	[A]
OS						
[IS] Servicios internos						
[E] Equipamiento						
[SS] Servicios subcontratados						
[023] [ADSL] Conexión a internet brindada por un ISP			50%			
[I.8] Fallo de servicios de comunicaciones		1,05	50%			
[E.2] Errores del administrador del sistema / de la seguridad		1,05	20%			
[E.18] Destrucción de la información		1,98	10%			
[E.24] Caída del sistema por agotamiento de recursos		1,98	50%			
[A.7] Uso no previsto		3,3	10%			
[A.18] Destrucción de la información		3,6	50%			
[A.24] Deneqación de servicio		33	50%			

Figura 23: amenazas sobre el activo [OFFICINA]



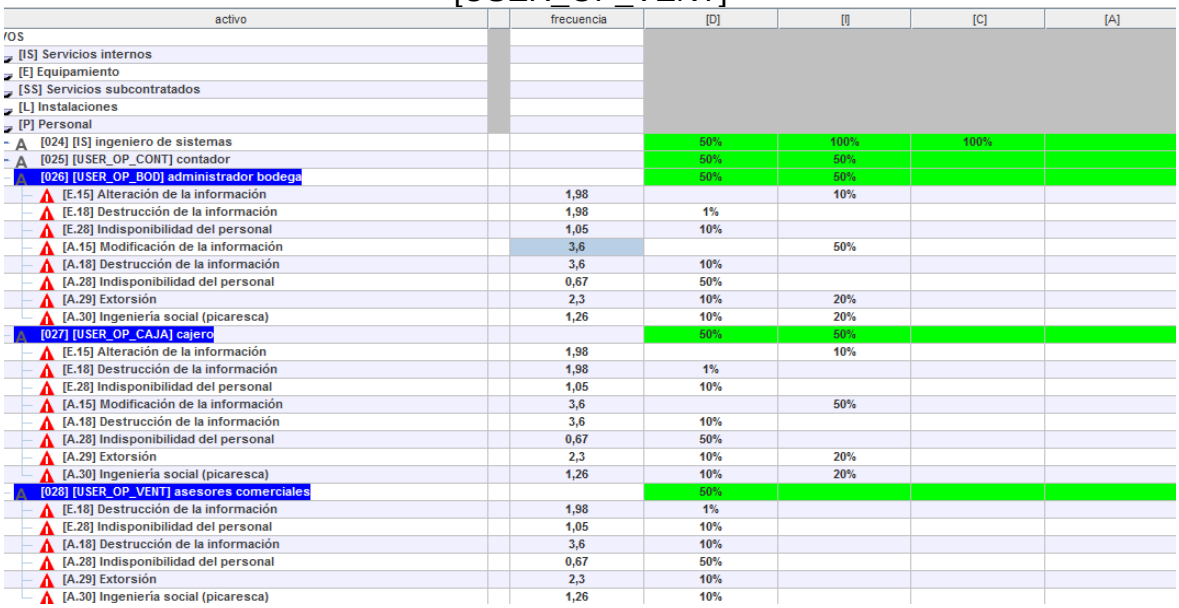
activo		frecuencia	[D]	[I]	[C]	[A]
S						
[IS] Servicios internos						
[E] Equipamiento						
[SS] Servicios subcontratados						
[L] Instalaciones						
[022] [oficina] CELUTEL SAS SINCELEJO CENTRO			100%			
[N.1] Fuego		1,05	100%			
[N.2] Daños por agua		1,05	100%			
[N.*] Desastres naturales		0,52	100%			
[I.1] Fuego		1,05	100%			
[I.2] Daños por agua		1,05	100%			
[I.*] Desastres industriales		1,05	100%			
[I.3] Contaminación medioambiental		1,05	10%			
[I.4] Contaminación electromagnética		0,105	10%			
[A.6] Abuso de privilegios de acceso		3,3	10%			
[A.7] Uso no previsto		3,3	10%			
[A.26] Ataque destructivo		0,147	100%			
[A.27] Ocupación enemiga		1,47	100%			

Figura 24: amenazas sobre el activos [IS] y [USER_OP_CONT]



activo		frecuencia	[D]	[I]	[C]	[A]
OS						
[IS] Servicios internos						
[E] Equipamiento						
[SS] Servicios subcontratados						
[L] Instalaciones						
[P] Personal						
[024] [IS] ingeniero de sistemas			50%	100%	100%	
[E.15] Alteración de la información		1,98		10%		
[E.18] Destrucción de la información		1,98	1%			
[E.19] Fugas de información		1,98			10%	
[E.28] Indisponibilidad del personal		1,05	10%			
[A.15] Modificación de la información		3,6		50%		
[A.18] Destrucción de la información		3,6	10%			
[A.19] Revelación de información		36			50%	
[A.28] Indisponibilidad del personal		0,67	20%			
[A.29] Extorsión		2,3	50%	100%	100%	
[A.30] Ingeniería social (picaresca)		1,26	50%	100%	100%	
[025] [USER_OP_CONT] contador			50%	50%		
[E.15] Alteración de la información		1,98		10%		
[E.18] Destrucción de la información		1,98	1%			
[E.28] Indisponibilidad del personal		1,05	10%			
[A.15] Modificación de la información		3,6		50%		
[A.18] Destrucción de la información		3,6	10%			
[A.28] Indisponibilidad del personal		0,67	50%			
[A.29] Extorsión		2,3	10%	20%		
[A.30] Ingeniería social (picaresca)		1,26	10%	20%		

Figura 25: amenazas sobre los activos [USER_OP_BOD], [USER_OP_CAJA] y [USER_OP_VENT]



activo		frecuencia	[D]	[I]	[C]	[A]
OS						
[IS] Servicios internos						
[E] Equipamiento						
[SS] Servicios subcontratados						
[L] Instalaciones						
[P] Personal						
[024] [IS] ingeniero de sistemas			50%	100%	100%	
[025] [USER_OP_CONT] contador			50%	50%		
[026] [USER_OP_BOD] administrador bodega			50%	50%		
[E.15] Alteración de la información		1,98		10%		
[E.18] Destrucción de la información		1,98	1%			
[E.28] Indisponibilidad del personal		1,05	10%			
[A.15] Modificación de la información		3,6		50%		
[A.18] Destrucción de la información		3,6	10%			
[A.28] Indisponibilidad del personal		0,67	50%			
[A.29] Extorsión		2,3	10%	20%		
[A.30] Ingeniería social (picaresca)		1,26	10%	20%		
[027] [USER_OP_CAJA] cajero			50%	50%		
[E.15] Alteración de la información		1,98		10%		
[E.18] Destrucción de la información		1,98	1%			
[E.28] Indisponibilidad del personal		1,05	10%			
[A.15] Modificación de la información		3,6		50%		
[A.18] Destrucción de la información		3,6	10%			
[A.28] Indisponibilidad del personal		0,67	50%			
[A.29] Extorsión		2,3	10%	20%		
[A.30] Ingeniería social (picaresca)		1,26	10%	20%		
[028] [USER_OP_VENT] asesores comerciales			50%			
[E.18] Destrucción de la información		1,98	1%			
[E.28] Indisponibilidad del personal		1,05	10%			
[A.18] Destrucción de la información		3,6	10%			
[A.28] Indisponibilidad del personal		0,67	50%			
[A.29] Extorsión		2,3	10%			
[A.30] Ingeniería social (picaresca)		1,26	10%			

Ante las evidencias presentadas por ear/pilar identificando las amenazas sobre los activos de CELUTEL SAS, se puede inferir que:

- Las bases de datos que almacenan la información contable y el registro de ventas las amenazas más frecuentemente presentadas son [A.19] Revelación de información y [A.24] Denegación de servicio, las cuales al

materializase afectarían la confidencialidad y la disponibilidad del activo para el cumplimiento del objeto de la empresa.

- En cuanto a los servicios internos de correo electrónico y servicio de internet la amenaza más relevante y frecuente es [A.24] Denegación de servicio, la cual afectaría directamente la disponibilidad del activo.

- Los activos de tipo software es notorio que la amenaza que con mayor frecuencia se presenta es [E.21] Errores de mantenimiento / actualización de programas (software), la cual afecta muy someramente la disponibilidad del activo, pero también se presenta la amenaza [A.24] Denegación de servicio, y en cuanto a esta ultima la afectación sobre la disponibilidad es total lo que ocasiona que el activo no estará disponible por un rango de tiempo considerable

- El análisis aplicado al activo servidor deja ver que las amenazas más altas son de tipo [E.24] Caída del sistema por agotamiento de recursos, [A.3] Manipulación de los registros de actividad (log) y [A.5] Suplantación de la identidad, las cuales al materializarse ocasionarían un daño grave al activo en 4 de sus dimensiones, las cuales son: disponibilidad, integridad, confidencialidad y autenticidad, lo que genera una gran pérdida en la información contenida en el servidor.

- En términos generales la amenaza más frecuente en los activos de tipo hardware [E.24] Caída del sistema por agotamiento de recursos, afectando directamente la disponibilidad del activo y aunque estos activos son fácilmente reemplazables (exceptuando el servidor), generarían perdida económicas y de información considerables.

- Los activos de comunicación posen una alta probabilidad de materialización de la amenaza [A.24] Denegación de servicio, la cual ocasiona un daño directo a la disposición de este activo lo que acarrea a la empresa demoras en todas sus operaciones debido a que se cuenta con un sistema manejado mediante las redes locales y con enlaces directos a través de internet para completar todas las actividades de la empresa tales como ventas en todas sus sedes y además con la plataforma de claro móvil la cual es accedida para el registro de las ventas de planes y equipos.

- En los activos de tipo personal tenemos dos grupos administrador del sistema y los operarios, en el caso del administrador (ingeniero de sistemas) encontramos que la amenaza más frecuente es [A.19] Revelación de información, la cual afecta en gran medida la confidencialidad de la información y además puede acarrear problemas graves debido a que de materializarse todo el sistema de información entraría en un estado de riesgo, en cuanto a los operativos (contador, caja, bodega y ventas) la amenaza más frecuente es [A.15] Modificación de la información, la cual afecta directamente la integridad de la información y ocasionando un gran daño a la información a la cual este activo tiene privilegios de acceder

6.6 ESTIMACIÓN DEL RIESGO

6.6.1 Impacto potencial acumulado: Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Para el cálculo del impacto acumulado se utiliza la siguiente formula

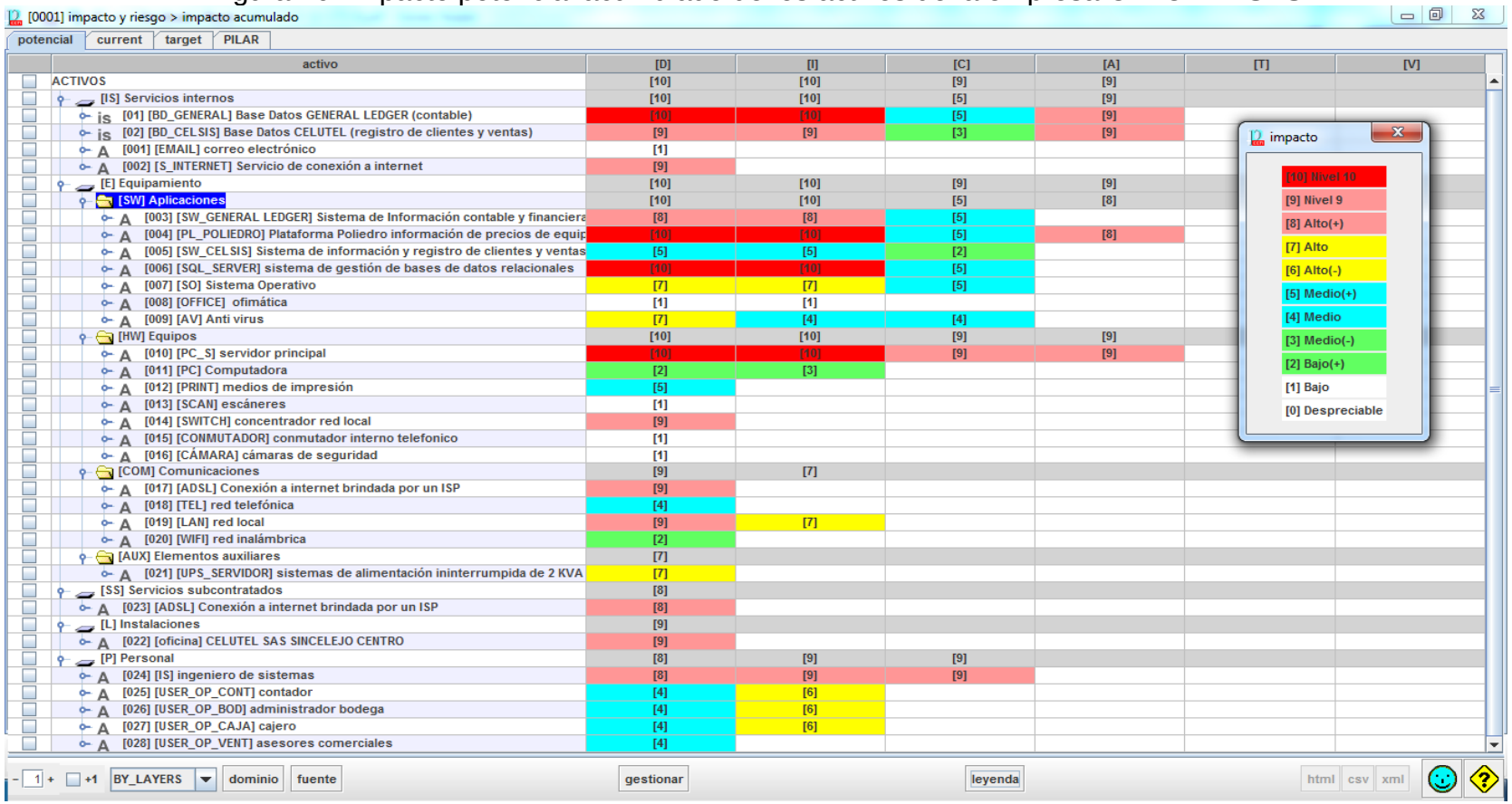
Impacto acumulado= valor acumulado * degradación

A cada dimensión se le realiza una valoración que depende de la materialización de una amenaza, es decir el valor que se obtiene en cada dimensión es el deterioro que tendrá la organización si un activo se ve dañado en una dimensión Para valorar las consecuencias de los criterios de valoración que utiliza la metodología y la herramienta PILAR son seis como se muestra en la siguiente tabla con su respectiva escala de valoración.

Tabla 7. Criterios de Valoración del impacto

VALOR		CRITERIO
10	EXTREMO	Daño extremadamente grave
9	MUY ALTO	Daño muy grave
8-6	ALTO (+)	Daño grave
	ALTO	
	ALTO (-)	
5-3	MEDIO (+)	Daño importante.
	MEDIO	
	MEDIO (-)	
2-1	BAJO (+)	Daño menor.
	BAJO	
0	DESPRECIABLE	Irrelevante a efectos prácticos.

Figura 26. Impacto potencial acumulado de los activos de la empresa CELUTEL SAS



La herramienta ear/pilar arroja los resultados del impacto acumulado de los activos de la empresa CELUTEL SAS, como se puede apreciar los activos más impactados son las bases de datos, los aplicativos contables y el motor de base de datos, además en la parte de hardware notamos que los activos servidor y el switch se encuentran en un estado muy alto, como también en los activos de comunicación notamos la red ADSL que es la que nos garantiza conexión a internet, además de eso es notorio que el activo ingeniero de sistemas está en un estado elevado.

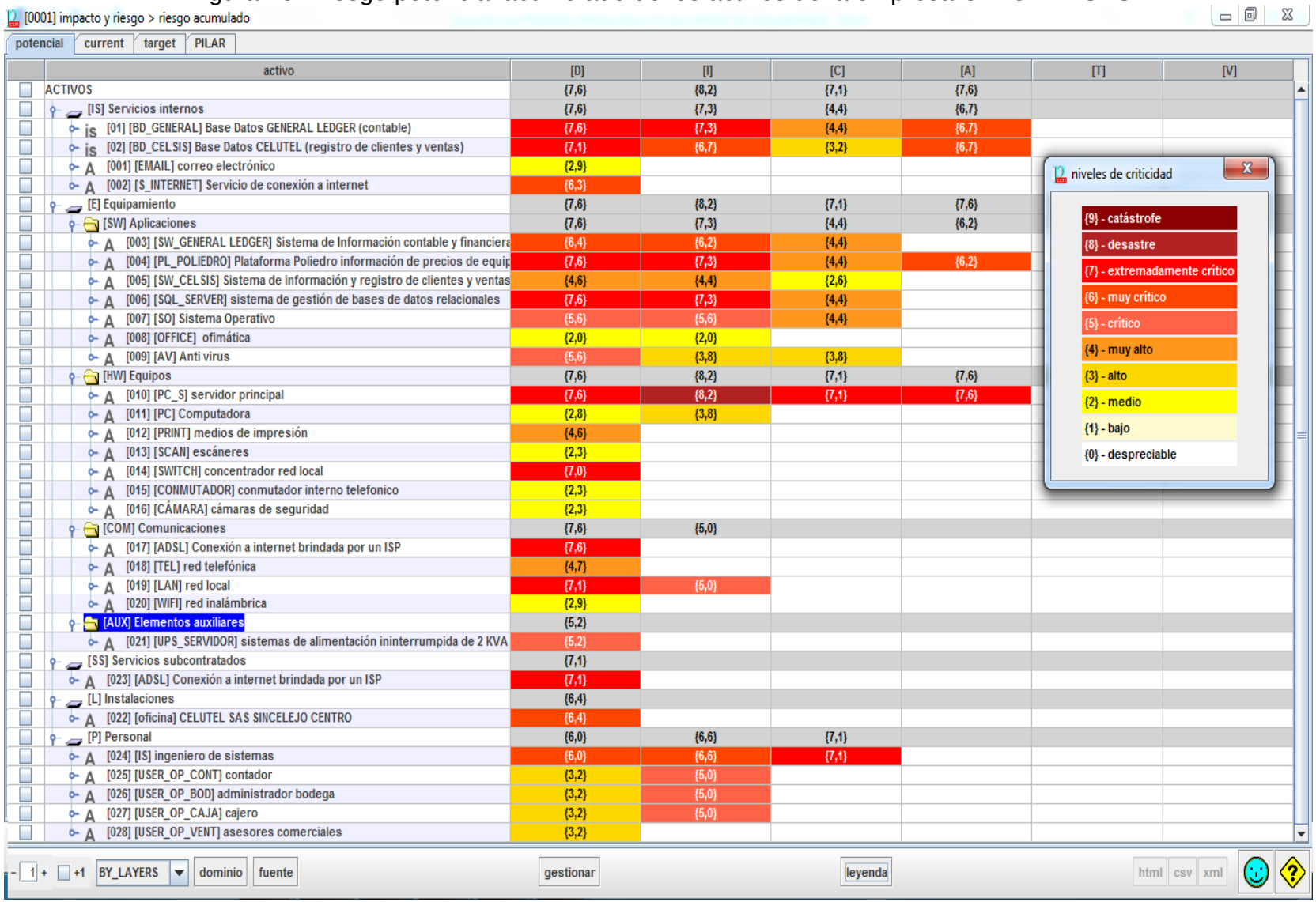
6.6.2 Riesgo potencial acumulado: El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la probabilidad de la amenaza. El riesgo acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

La herramienta pilar ofrece ciertos niveles de criticidad tal cual lo representa la siguiente imagen.

Figura 27. Niveles de criticidad ear/pilar

A continuación se muestra el estado de los activos en lo pertinente a los riesgos potenciales acumulados, datos obtenidos mediante la implementación de la herramienta ear/pilar.

Figura 28. Riesgo potencial acumulado de los activos de la empresa CELUTEL SAS



activo	[D]	[I]	[C]	[A]	[T]	[V]
ACTIVOS	{7,6}	{8,2}	{7,1}	{7,6}		
[IS] Servicios internos	{7,6}	{7,3}	{4,4}	{6,7}		
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	{7,6}	{7,3}	{4,4}	{6,7}		
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	{7,1}	{6,7}	{3,2}	{6,7}		
[001] [EMAIL] correo electrónico	{2,9}					
[002] [S_INTERNET] Servicio de conexión a internet	{6,3}					
[E] Equipamiento	{7,6}	{8,2}	{7,1}	{7,6}		
[SW] Aplicaciones	{7,6}	{7,3}	{4,4}	{6,2}		
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	{6,4}	{6,2}	{4,4}			
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equip	{7,6}	{7,3}	{4,4}	{6,2}		
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	{4,6}	{4,4}	{2,6}			
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	{7,6}	{7,3}	{4,4}			
[007] [SO] Sistema Operativo	{5,6}	{5,6}	{4,4}			
[008] [OFFICE] ofimática	{2,0}	{2,0}				
[009] [AV] Anti virus	{5,6}	{3,8}	{3,8}			
[HW] Equipos	{7,6}	{8,2}	{7,1}	{7,6}		
[010] [PC_S] servidor principal	{7,6}	{8,2}	{7,1}	{7,6}		
[011] [PC] Computadora	{2,8}	{3,8}				
[012] [PRINT] medios de impresión	{4,6}					
[013] [SCAN] escáneres	{2,3}					
[014] [SWITCH] concentrador red local	{7,0}					
[015] [CONMUTADOR] conmutador interno telefonico	{2,3}					
[016] [CÁMARA] cámaras de seguridad	{2,3}					
[COM] Comunicaciones	{7,6}	{5,0}				
[017] [ADSL] Conexión a internet brindada por un ISP	{7,6}					
[018] [TEL] red telefónica	{4,7}					
[019] [LAN] red local	{7,1}	{5,0}				
[020] [WIFI] red inalámbrica	{2,9}					
[AUX] Elementos auxiliares	{5,2}					
[021] [UPS_SERVIDOR] sistemas de alimentación ininterrumpida de 2 KVA	{5,2}					
[SS] Servicios subcontratados	{7,1}					
[023] [ADSL] Conexión a internet brindada por un ISP	{7,1}					
[L] Instalaciones	{6,4}					
[022] [oficina] CELUTEL SAS SINCELEJO CENTRO	{6,4}					
[P] Personal	{6,0}	{6,6}	{7,1}			
[024] [IS] ingeniero de sistemas	{6,0}	{6,6}	{7,1}			
[025] [USER_OP_CONT] contador	{3,2}	{5,0}				
[026] [USER_OP_BOD] administrador bodega	{3,2}	{5,0}				
[027] [USER_OP_CAJA] cajero	{3,2}	{5,0}				
[028] [USER_OP_VENT] asesores comerciales	{3,2}					

Para comprender la imagen anterior debemos tener claridad de cuáles son sus parámetros manejados por la herramienta ear/pilar para realizar los cálculos, a continuación se presentan los parámetros:

- **Activos:** representa el activo que va a ser valorado.

- **Amenaza:** amenazas que afectan al activo (metodología Magerit).

- **Dimensión:** las definidas por la mitología Magerit estas son: [D] disponibilidad, [I] integridad, [C] Confidencialidad, [A] Autenticidad y [T] Trazabilidad.

- **V (Valor):** representa el valor que se le dio al activo.

- **VA (Valor acumulado):** representa el valor acumulado del activo (la suma del valor del propio activo más el valor de los activos que dependen de él.)

- **D (Degradación):** representa la degradación que le provoca la amenaza al activo.

- **I (Impacto):** representa el impacto que le provoca la materialización de la amenaza al activo.

- **Frecuencia:** representa la frecuencia o estimación con la que se puede materializar una amenaza.

En la tabla presentada a continuación veremos un ejemplo del riesgo acumulado que tiene el activo servidor, la tabla completa se encuentra en el ANEXO C (tabla de riesgos potenciales de los activos de CELUTEL SAS); en ella se puede evidenciar que se en un nivel crítico:

Tabla 8. Resumen Riesgo acumulado del activo servidor

Activo	Amenaza	Dimensión	V	VA	D	I	F	Riesgo
[010] [PC_S]	[N.1] Fuego	[D]	[10]	[10]	100%	[10]	0,105	{6,0}
[010] [PC_S]	[N.2] Daños por agua	[D]	[10]	[10]	50%	[9]	0,105	{5,4}
[010] [PC_S]	[N.*] Desastres naturales	[D]	[10]	[10]	100%	[10]	0,105	{6,0}
[010] [PC_S]	[I.1] Fuego	[D]	[10]	[10]	100%	[10]	0,52	{6,6}
[010] [PC_S]	[I.2] Daños por agua	[D]	[10]	[10]	50%	[9]	0,52	{6,1}
[010] [PC_S]	[I.*] Desastres industriales	[D]	[10]	[10]	100%	[10]	0,52	{6,6}
[010] [PC_S]	[I.3] Contaminación medioambiental	[D]	[10]	[10]	50%	[9]	0,105	{5,4}
[010] [PC_S]	[I.4] Contaminación electromagnética	[D]	[10]	[10]	10%	[7]	1,05	{5,1}
[010] [PC_S]	[I.5] Avería de origen físico o lógico	[D]	[10]	[10]	50%	[9]	1,05	{6,3}
[010] [PC_S]	[I.6] Corte del suministro eléctrico	[D]	[10]	[10]	100%	[10]	1,05	{6,9}
[010] [PC_S]	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[10]	[10]	100%	[10]	1,05	{6,9}
[010] [PC_S]	[I.11] Emanaciones electromagnéticas	[C]	[9]	[9]	1%	[3]	1,05	{2,7}
[010] [PC_S]	[E.3] Errores de monitorización (log)	[I]	[10]	[10]	1%	[4]	1,05	{3,3}
[010] [PC_S]	[E.8] Difusión de software dañino	[C]	[9]	[9]	10%	[6]	1,98	{4,7}
[010] [PC_S]	[E.8] Difusión de software dañino	[D]	[10]	[10]	10%	[7]	1,98	{5,3}
[010] [PC_S]	[E.8] Difusión de software dañino	[I]	[10]	[10]	10%	[7]	1,98	{5,3}
[010] [PC_S]	[E.15] Alteración de la información	[I]	[10]	[10]	1%	[4]	1,98	{3,6}
[010] [PC_S]	[E.18] Destrucción de la información	[D]	[10]	[10]	1%	[4]	1,98	{3,6}
[010] [PC_S]	[E.20] Vulnerabilidades de los programas (software)	[I]	[10]	[10]	20%	[8]	1,05	{5,6}

[010] [PC_S]	[E.20] Vulnerabilidades de los programas (software)	[D]	[10]	[10]	1%	[4]	1,05	{3,3}
[010] [PC_S]	[E.20] Vulnerabilidades de los programas (software)	[C]	[9]	[9]	20%	[7]	1,05	{5,0}
[010] [PC_S]	[E.21] Errores de mantenimiento / actualización de programas (software)	[D]	[10]	[10]	1%	[4]	19,8	{4,4}
[010] [PC_S]	[E.21] Errores de mantenimiento / actualización de programas (software)	[I]	[10]	[10]	1%	[4]	19,8	{4,4}
[010] [PC_S]	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D]	[10]	[10]	10%	[7]	1,98	{5,3}
[010] [PC_S]	[E.24] Caída del sistema por agotamiento de recursos	[D]	[10]	[10]	50%	[9]	19,8	{7,4}
[010] [PC_S]	[E.25] Pérdida de equipos	[C]	[9]	[9]	100%	[9]	1,98	{6,5}
[010] [PC_S]	[E.25] Pérdida de equipos	[D]	[10]	[10]	100%	[10]	1,98	{7,1}
[010] [PC_S]	[A.3] Manipulación de los registros de actividad (log)	[I]	[10]	[10]	50%	[9]	147	{8,2}
[010] [PC_S]	[A.5] Suplantación de la identidad	[A]	[9]	[9]	100%	[9]	36	{7,6}
[010] [PC_S]	[A.5] Suplantación de la identidad	[I]	[10]	[10]	10%	[7]	36	{6,4}
[010] [PC_S]	[A.5] Suplantación de la identidad	[C]	[9]	[9]	50%	[8]	36	{7,1}
[010] [PC_S]	[A.6] Abuso de privilegios de acceso	[C]	[9]	[9]	50%	[8]	33	{7,1}
[010] [PC_S]	[A.6] Abuso de privilegios de acceso	[D]	[10]	[10]	1%	[4]	33	{4,6}
[010] [PC_S]	[A.6] Abuso de privilegios de acceso	[I]	[10]	[10]	10%	[7]	33	{6,4}
[010]	[A.7] Uso no previsto	[C]	[9]	[9]	10%	[6]	3,3	{4,9}

[PC_S]								
[010] [PC_S]	[A.7] Uso no previsto	[I]	[10]	[10]	1%	[4]	3,3	{3,8}
[010] [PC_S]	[A.7] Uso no previsto	[D]	[10]	[10]	1%	[4]	3,3	{3,8}
[010] [PC_S]	[A.8] Difusión de software dañino	[D]	[10]	[10]	100%	[10]	3,6	{7,3}
[010] [PC_S]	[A.8] Difusión de software dañino	[C]	[9]	[9]	100%	[9]	3,6	{6,7}
[010] [PC_S]	[A.8] Difusión de software dañino	[I]	[10]	[10]	100%	[10]	3,6	{7,3}
[010] [PC_S]	[A.11] Acceso no autorizado	[D]	[10]	[10]	10%	[7]	3,6	{5,6}
[010] [PC_S]	[A.11] Acceso no autorizado	[I]	[10]	[10]	10%	[7]	3,6	{5,6}
[010] [PC_S]	[A.11] Acceso no autorizado	[C]	[9]	[9]	50%	[8]	3,6	{6,2}
[010] [PC_S]	[A.22] Manipulación de programas	[C]	[9]	[9]	100%	[9]	3,3	{6,7}
[010] [PC_S]	[A.22] Manipulación de programas	[D]	[10]	[10]	50%	[9]	3,3	{6,8}
[010] [PC_S]	[A.22] Manipulación de programas	[I]	[10]	[10]	100%	[10]	3,3	{7,3}
[010] [PC_S]	[A.23] Manipulación del hardware	[C]	[9]	[9]	50%	[8]	0,74	{5,6}
[010] [PC_S]	[A.23] Manipulación del hardware	[D]	[10]	[10]	50%	[9]	0,74	{6,2}
[010] [PC_S]	[A.24] Denegación de servicio	[D]	[10]	[10]	100%	[10]	6,6	{7,6}
[010] [PC_S]	[A.25] Robo de equipos	[C]	[9]	[9]	100%	[9]	0,74	{6,1}
[010] [PC_S]	[A.25] Robo de equipos	[D]	[10]	[10]	100%	[10]	0,74	{6,7}
[010] [PC_S]	[A.26] Ataque destructivo	[D]	[10]	[10]	100%	[10]	1,47	{7,0}

Para la obtención de estos datos se utilizó la herramienta ear/pilar.

6.7 IDENTIFICACIÓN DE SALVAGUARDAS

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieres elementos técnicos

(programas o equipos), otra seguridad física y, por último, está la política de personal.

Las salvaguardas y los grupos de salvaguardas en ear/pilar están identificadas por un icono en forma de paraguas y un subíndice. Los colores y valores subíndice de los paraguas informan de la importancia relativa de la salvaguarda, que puede ser:

Figura 29. Salvaguardas en ear/pilar

-  : Interesante.
-  Importante.
-  : Muy importante.
-  : Crítica.

El resultado obtenido mediante el programa ear/pilar, señala una serie de aspectos y estrategias, los cuales debemos tener claros para la interpretación del resultado y estas son:

- **Aspectos :**
  - ✓ G: Gestión.
  - ✓ T: Técnico.
  - ✓ P: Personal.
  - ✓ F: Seguridad física.

- **Estrategia**: representa la estrategia que toma la salvaguarda frente a los incidentes para mitigarlos o eliminarlos; dentro de ellas tenemos los siguientes valores:

- ✓ **CR** (Corrección): Se parte de que ya se produjo un daño y debe ser corregido o reparado.

- ✓ **EL** (Eliminación): actúa antes de que el incidente ocurra e impide que este tenga lugar en sistema de información.

- ✓ **PR** (Prevención): es preventiva cuando se reducen las oportunidades de que un incidente ocurra.

- ✓ **IM** (Minimización / limitación del impacto): Se dice que se minimiza el impacto cuando limita las consecuencias de un incidente.
- ✓ **DR** (Disuasión): este valor nos indica que genera un efecto tal sobre los atacantes que logra que ellos no se atrevan a atacar al sistema.

- ✓ **DT** (Detección): funciona detectando un ataque e informando de que este está ocurriendo; permitiendo que entren en operación otras medidas que mitiguen la progresión del ataque, minimizando daños.

- ✓ **RC** (Recuperación): Se ofrece recuperación cuando permite regresar al estado anterior al incidente.

- ✓ **MN** (Monitorización): como su nombre lo indica trabajan monitorizando lo que está ocurriendo reaccionando ante un incidente limitando su impacto.

- ✓ **AW** (Concienciación): son las capacitaciones de las personas que interactúan con el sistema teniendo como objetivo la reducción de los errores de los mismos, lo cual tiene un efecto preventivo.

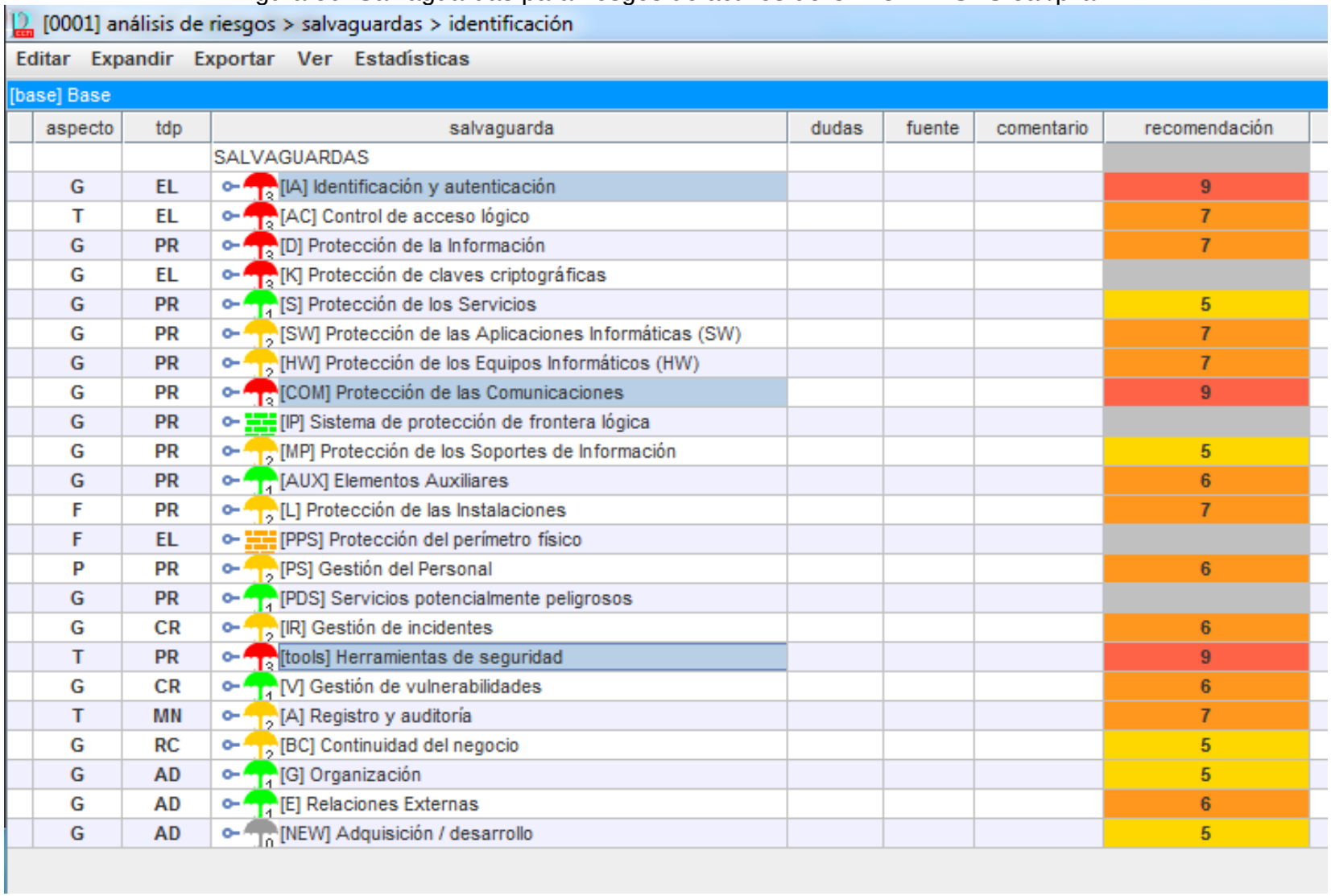
- ✓ **AD** (Administración): se refiere a la administración de los componentes de seguridad del sistema. Tiene como objetivo evitar dejar puertas abiertas que permitan el éxito de un ataque.

- ✓ **STD** (Normativa, Standard): Se refiere a las salvaguardas basadas en normas.

- ✓ **PROC** (Procedimiento de seguridad): Se refiere a las salvaguardas basadas en procedimientos.

- ✓ **CERT** (Producto certificado): Se refiere a las salvaguardas basadas en productos certificados.

Figura 30. Salvaguardas para riesgos de activos de CELUTEL SAS ear/pilar



[0001] análisis de riesgos > salvaguardas > identificación

Editar Expandir Exportar Ver Estadísticas

[base] Base

aspecto	tdp	salvaguarda	dudas	fuente	comentario	recomendación
		SALVAGUARDAS				
G	EL	[IA] Identificación y autenticación				9
T	EL	[AC] Control de acceso lógico				7
G	PR	[D] Protección de la Información				7
G	EL	[K] Protección de claves criptográficas				
G	PR	[S] Protección de los Servicios				5
G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)				7
G	PR	[HW] Protección de los Equipos Informáticos (HW)				7
G	PR	[COM] Protección de las Comunicaciones				9
G	PR	[IP] Sistema de protección de frontera lógica				
G	PR	[MP] Protección de los Soportes de Información				5
G	PR	[AUX] Elementos Auxiliares				6
F	PR	[L] Protección de las Instalaciones				7
F	EL	[PPS] Protección del perímetro físico				
P	PR	[PS] Gestión del Personal				6
G	PR	[PDS] Servicios potencialmente peligrosos				
G	CR	[IR] Gestión de incidentes				6
T	PR	[tools] Herramientas de seguridad				9
G	CR	[V] Gestión de vulnerabilidades				6
T	MN	[A] Registro y auditoría				7
G	RC	[BC] Continuidad del negocio				5
G	AD	[G] Organización				5
G	AD	[E] Relaciones Externas				6
G	AD	[NEW] Adquisición / desarrollo				5

Como es notorio en la imagen anterior se deben tomar medidas urgentes sobre la autenticación e identificación del personal que accede a la información, además incrementar la protección de las comunicaciones previniendo sobre ella daños que generen perdida de la información y evite el buen funcionamiento de la empresa, además se debe hacer inca pie en establecer herramientas de seguridad sobre los activos de la empresa

7. CONCLUSIONES

Con el desarrollo de este proyecto se obtuvo claridad sobre la situación actual de la empresa CELUTEL SAS, la cual en este momento tiene su sistema de información completamente expuesto a amenazas, lo que la vuelve vulnerable, además de ello es notorio que no posee ningún control eficiente en su sistema y que los activos no reciben la importancia que deben, con la implementación de MAGERIT se obtuvo una identificación de cada activo y de él se definieron amenazas potenciales, los impactos y riesgos a los cuales se exponen, definiendo para ellos salvaguardas logrando la mitigación en caso de la materialización de la amenaza, con ello se llevó a CELUTEL SAS a un estado más seguro de su sistema de información.

La identificación de los activos es una fase fundamental para el análisis de riesgo debido a que en esta fase se obtiene claridad sobre cada uno de los elementos que conforman el sistema de información, además de ello identificar cada una de las amenazas que sobre estos activos recae es de vital importancia ya que sobre ellas es donde se presentan los riegos si su materialización se presenta, y como la metodología lo indica se deben definir salvaguardas que permitan tratar el riesgo potencial, lo que lograra mantener el sistema de información protegido y a salvo de riesgos.

Luego de realizar el análisis de riesgo a la empresa es indispensable la aplicación de un plan de seguridad, en este caso luego del análisis se propone un plan de seguridad que brindara a la empresa un nivel más elevado de su sistema de seguridad informática, además garantiza que los activos tenga el manejo adecuado y se previene la materialización de amenazas que en la actualidad tienen un alto grado de posible materialización

El principal riesgo notado y tratado es el personal el cual en estos momentos no tiene un conocimiento ideal de lo que comprende el sistema de información y los cuidados a tener sobre él, además los procesos de inducción y re inducción son inexistentes lo que ocasiona que los empleados para la solución de problemas y manejo de la información lo hagan a criterio propio lo que no en todo caso presenta la seguridad que amerita

8. RECOMENDACIONES

Se recomienda el acatamiento de lo dispuesto por este proyecto a la gerencia de la empresa CELUTEL SAS, y lograr con ello llevar al sistema de seguridad de la información a un estado aceptable.

Para que la empresa continúe las operaciones sin inconvenientes se recomienda la implementación de un sistema de mejora continua que se ligue a las recomendaciones establecidas en este trabajo y vincule el análisis de riesgos, y auditorías internas sobre el sistema de seguridad y la implementación de todas las políticas fijadas en la empresa.

Implementar sistemas de capacitaciones y de divulgación de la información con el fin de mantener el personal siempre actualizado y cumpliendo con las normas que aumentan su seguridad y la seguridad del sistema.

Dar continuidad al proceso de análisis de riesgo implementar los salvaguardas sugeridos y realizar una análisis constante sobre las nuevas situaciones presentadas con el fin de mantener siempre el sistema de información funcionando de una forma eficiente y protegido

BIBLIOGRAFÍA

Dirección de Estándares y Arquitectura de TI del Ministerio de las Tecnologías de Información y las Comunicaciones de la República de Colombia. (2014). Generalidades del Marco de Referencia– versión 1.0. Disponible en URL: http://www.mintic.gov.co/marcodereferencia/624/articles-8102_generalidades.pdf

García Guevara C.A. (2012). Establecimiento del sistema de seguridad de información en SFG bajo los estándares de la norma ISO 27001: 2005 - Informe final de investigación. Universidad EAN. Disponible en URL: http://repository.ean.edu.co/handle/10882/1457/browse?value=Garc%C3%ADa+Guevara% 2C+Camilo+Augusto&type=author.

Icontec internacional. (2013). NTC- ISO 27001. Sistemas de gestión de la Información Editada por el Instituto de Normas Técnicas y Certificación (ICONTEC): Autor.

COBIT. ISACA Trust in, and value from, information systems. [En línea].

https://www.isaca.org/Pages/default.aspx. Marco de referencia para optimizar y salvaguardas los recursos o activos de información y tecnológicos de cualquier empresa.

González Barroso, J. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid. Ministerio de Hacienda y Administraciones Públicas. Libro I de la metodología Magerit ofrece los lineamientos necesarios en el Proceso de Gestión de Riesgos dentro de un marco de trabajo para administrar los riesgos derivados del uso de tecnologías de la información.

González Barroso, Jesús. (2012). Guía de Técnicas. Madrid. Ministerio de Hacienda y Administraciones Públicas. Libro III de la metodología Magerit describe las técnicas usadas para hacer el Análisis de riesgos.

González Barroso, Jesús. (2012). Catálogo de Elementos. Madrid. Ministerio de

Hacienda y Administraciones Públicas. (v.3.0): Metodología de análisis y Gestión de riesgos los sistemas de información. Libro número II de la metodología MAGERIT, estandariza los elementos objeto de proyecto de análisis necesarios para generar un inventario de activos, para luego hacer la administración de estos.

Portal administración electrónica. MAGERIT v3: Metodología de Análisis y Gestión de Riesgos de los sistemas de información. [En línea]. http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VCmVZhZRVJQ.

SANDOVAL VARGAS, Cesar Andrés. Análisis de la norma ISO/IEC 27001. Diseño de Implementación en la red de una empresa. Guayaquil, 2014, 174p. Tesis posgrado (Magíster en telecomunicaciones). Universidad Católica de Santiago de Guayaquil {en línea}. disponible en: (http://repositorio.ucsg.edu.ec/bitstream/123456789/1937/1/T-UCSG-POS-MTEL-16.pdf).

PALLAS MEGA, Gustavo. Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. Montevideo, 2009, 195p. Tesis de Maestría (Magíster en Ingeniería de Computación). Institución de Computación. Facultad de Ingeniería. {en línea} disponible en: (http://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf)

ANGULO, Maire y ANGULO RODRIGUEZ, Jaime. Diseño del Sistema de Gestión de la Seguridad de la información en la Empresa Bohórquez Metalmecánica Industrial Ltda. Basados en la Norma ISO 27001 {en línea}.{20 de Marzo de 2016} Disponible en: (http://www.uan.edu.co/images/programasposgrados/Esp_Auditoria_sistemas/documentos/2011_II/DISE%C3%91O_DEL_SISTEMA_DE_GESTI%C3%93N_DE_LA_SEGURIDAD_DE_LA_INFORMACI%C3%93N_EN_LA_EMPRESA_BOH%C3%93RQUEZ_METALMEC%C3%81NICA_INDUSTRIAL_LTDA._BASADOS_EN_LA_NORMA_ISO_27001.pdf)

MENDOZA, Miguel. Primeros pasos hacia la implementación de ISO/IEC 27001 {en línea}.{20 de Marzo de 2016} Disponible en (http://www.welivesecurity.com/la-es/2014/08/20/como-iniciar-implementacion-iso-27001/)

CORPORACIÓN COLOMBIA DIGITAL. Empresas colombianas no están preparada antes Riesgos Informáticos. {en línea}.{20 de Marzo de 2016} Disponible en (www.colombiadigital.net/actualidad/noticias/item/8168-organizaciones-colombianas-no-estan-preparadas-ante-riesgos-informaticos.html)

Administración de riesgos: Metodología NIST 800-30 {en línea}.{20 de Marzo de 2016} disponible en (http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)

CHICANO, Ester. MF0490_3: Gestión de servicios en el sistema informático: Certificado de Profesionalidad IFCT0509 - Administración de servicios de internet. ANTEQUERA, Málaga: IC Editorial, 2014, 330p. {en línea}.{20 de Marzo de 2016} Disponible en (https://books.google.com.co/books?id=Oq7KCQAAQBAJ&pg=PT275&dq=activo+informatico&hl=es&sa=X&ved=0CB8Q6AEwAWoVChMIlsuhnJTeyAIVhdceCh2Ipwcp#v=onepage&q&f=false)

BSIGROUP. Guía de transición: Pasando del estándar de ISO/IEC 27001:2005 A ISO/IEC 27001:2013 {en línea}.{20 de Marzo de 2016} Disponible en (http://www.bsigroup.com/LocalFiles/es-MX/ISO%20IEC%2027001/Gu%C3%ADa%20de%20Transici%C3%B3n_ISO27001.pdf)

FRANCO, Diana y GUERRERO, Cesar. Sistema de Administración de controles de seguridad informática basado en ISO/IEC 27002 {en línea}.{20 de Marzo de 2016} Disponible en (http://www.laccei.org/LACCEI2013-Cancun/RefereedPapers/RP239.pdf)

COLOMBIA. PRESIDENTE DE LA REPUBLICA DE COLOMBIA. Decreto 460 de 1995 por el cual se reglamenta el Registro Nacional del Derecho de Autor y se regula el Depósito Legal. {en línea}.{20 de Marzo de 2016} Disponible en (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=10576)

COLOMBIA. LA COMISION DEL ACUERDO DE CARTAGENA. Decisión 351 de la C.A.N por el cual decide: REGIMEN COMÚN SOBRE DERECHO DE AUTOR Y

DERECHOS CONEXOS{en línea}.{20 de Marzo de 2016} Disponible en (http://www.sice.oas.org/trade/junac/decisiones/dec351s.asp)

MAGERIT- versión 3.0. Metodología de Análisis y Gestión de Riesgos de los sistemas de Información. Madrid, octubre de 2012, Libro I - Método, NIPO 630-12-171-8

KASSE INITIATIVES. Systems Architectures. {en línea}.{20 de Marzo de 2016} Disponible en: (http://www.dtic.mil/ndia/2004cmmi/CMMIT1Mon/Track1IntrotoSystemsEngineering/ KISE07SystemsArchitecturesv2.pdf)

UNIVERSIDAD DE MURCIA. Concepto de datos.{en línea}.{20 de Marzo de 2016} Disponible en http://www.um.es/docencia/pguardio/documentos/Tec3.pdf

DUQUE OLIVA, Edison Jair. Revisión del concepto de calidad del servicio y sus modelos de medición. en: INNOVAR. (Enero a Junio. 2005). p. 64-80. {en línea}.{20 de Marzo de 2016} Disponible en (http://www.scielo.org.co/pdf/inno/v15n25/v15n25a04.pdf)

GUIMI. Redes de comunicaciones. {en línea}.{20 de Marzo de 2016} Disponible en http://guimi.net/monograficos/G-Redes_de_comunicaciones/G-Redes_de_comunicaciones.pdf.

ALVAREZ BASALDÚA, Luis Daniel. SEGURIDAD EN INFORMÁTICA (AUDITORÍA EN SISTEMAS). México D.F., 2005, 117p. Tesis Posgrado (MAESTRO EN INGENIERIA DE SISTEMAS EMPRESARIALES). Universidad Iberoamericana {en línea}. Disponible en: (http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf)

ICONTEC INTERNACIONAL. Guía Técnica GTC-ISO/IEC COLOMBIANA 27002 {en línea}.{12 de Mayo de 2016} Disponible en (http://bibliotecavirtual.unad.edu.co:2083/icontec_enormas_mobile/visor/HTML5.asp)

JALAL FEGHHI, JALIL FEGHHI Y PETER WILLIAM. DIGITAL CERTIFICATES, Applied Internet Security. ISBN: 0-201-30980-7. Editorial: Addison-Wesley - 1998 -

453 {en línea}{29 de Mayo de 2016}(páginasShttp://revistasic.com/revista39/pdf_39/SIC_39_bibliografia.PDF).

ENTRUST. Authority PKI, An Integrated Security Infrastructure for Encryption, Digital Signatures & Certificate Authentication {en línea}{29 de Mayo de 2016} (https://www.entrust.com/products/entrust-authority-pki/)

ANEXO A.

Carta Autorización Celutel

Celutel S.A.S. DISTRIBUIDOR AUTORIZADO

Claro

Sincelejo, 19 de Febrero 2016

Estimados Ingenieros UNAD

Por medio de la presente me permito autorizar a los estudiantes de Especialización en Seguridad Informática **JOSE LUIS PIEDRAHITA TATIS** identificado con cedula de ciudadania **92.556513** y **MOSHE AARON BOSSA CASTRO** identificado con cedula de ciudadania **CC 1.103.104.898** para hacer el estudio necesario y uso de la información interna de **Celutel S.A.S** para fines Académicos haciendo una propuesta de grado en la parte de AUDITORIA A LA SEGURIDAD INFORMATICA Y DE LA INFORMACION DE LA EMPRESA.

Este permiso será efectivo hasta diciembre 5 del año en curso por cuestiones de Logística.

Atentamente,

Mirley Escamilla

Administradora

Celutel S.A.S. N.T. 823.004.363-2

ANEXO B.

POLÍTICAS DE SEGURIDAD

En esta política es centrada en los principios que consagran las dimensiones de valoración de un activo ellas son, disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad, y su fin último es brindar la protección requerida por el sistema de información que maneja la empresa CELUTEL SAS, y así blindarlo tanto de amenazas internas como externas

Política general del manejo de activos de información.

Objetivo: obtener herramientas para el manejo de la información en la empresa CELUTEL SAS, enfocadas al buen uso y seguridad del sistema de información.

Aplicabilidad: esta política es aplicada a todo el personal, denomínese este administrativo, operativo y contratistas, en general se aplica a todo el personal que tenga contacto con el sistema de información de CELUTEL SAS

Directrices:

- Creación e implementación de manual de funciones, en los cuales se defina claramente las funciones y alcance de cada uno de los perfiles con los que cuenta la empresa.

- Definir cláusulas de confidencialidad y aplicarla a los contratos dependiendo del perfil contratado asegurando con ello que el personal se abstenga de filtrar información que puede ser vital para la empresa.

- Crear y aplicar manual de inducción y re-inducción, especificando en el todos los parámetros de seguridad pertinentes a manejo de la información, contraseñas y acceso a zonas no permitidas dependiendo del perfil del empleado.

- Implementación del sistema contra incendio, ubicar extintores den las zonas más propensas a incendios y capacitar a todo el personal sobre su manejo, además de ello programar revisión anual de todo el sistema contra incendios e incluir capacitaciones sobre su manejo.

- Programar mantenimientos preventivos y correctivos de ser necesarios sobre el sistema de cómputo cada 6 meses, y además sobre el sistema de aires acondicionados y eléctricos de la empresa.

- Mantener segmentada las redes de datos para garantizar el buen funcionamiento y continuidad del servicio.

Política de Recurso Humano (personal)

Objetivo: brindar al personal los conocimientos necesarios para el buen manejo del sistema de información y comprometerlos con su buen uso.

Aplicabilidad: esta política es aplicada a todo el personal, denomínese este administrativo, operativo y contratistas, en general se aplica a todo el personal que tenga contacto con el sistema de información de CELUTEL SAS

Directrices:

- Implementar procesos de capacitación sobre el sistema de seguridad informática manejado en la empresa, siendo claros en establecer las restricciones y cuidados que se deben tener en el manejo de la información de la empresa y su ciclo normal de fluencia, logrando con ello que el personal se entere de la dirección hacia cual se mueve la información y los responsables de su manejo, además de capacitaciones de seguridad al administrador del sistema con el fin de mantenerlo actualizado sobre los nuevos riesgos de seguridad informática.

- Instituir compromisos de confidencialidad con todo el personal de la empresa, como también las restricciones que de acceso que tendrá y las políticas de manejo de contraseña establecidas por la organización.

- Crear espacios de socialización y análisis del sistema de seguridad informática, en los cuales el personal en general tendrá una participación activa en la cual mostraran los incidentes presentados, y las debilidades del sistema que han notado, todo ello con el fin de fortificar la seguridad mitigando los efectos producidos y evitando que vuelvan a suceder.

- En caso de despido el empleado debe entregar todos los recursos suministrados por la empresa y que hagan parte de su funcionamiento, como también las contraseñas tanto de correo como de acceso al equipo de trabajo de la empresa, además de ello el administrador de sistemas deberá realizar la suspensión del usuario de correo y equipo para evitar fugas de información.

- En caso de daño o falla de un activo el usuario no debe tomar decisiones para intentar reparar el problema, se debe notificar al área correspondiente en este caso al encargado de sistemas.

- El empleado en su área de trabajo no debe dejar el equipo desbloqueado en caso de ausencia corta, así mismo cuando termine su horario laboral debe finalizar la sesión y apagar el mismo.

- Mantener el área de escritorio libre con el fin de evitar cualquier pérdida de información o manipulación por un tercero.

Política de accesos al sistema de información

Objetivo: garantizar la seguridad de la información y el acceso a la misma por todos y cada uno de los usuarios.

Aplicabilidad: esta política es aplicada a todo el personal, denomínese este administrativo, operativo y contratistas, en general se aplica a todo el personal que tenga contacto con el sistema de información de CELUTEL SAS

Directrices:

- Implementación del servidor de dominio: con el fin de garantizar la autenticación de cada uno de los usuarios del sistema, así se mantendrá el control sobre cada uno de los empleados.

- Establecer perfiles de seguridad robustos con identificación única de empleado, en los cuales los permisos y restricciones se enmarquen en el rol que jugara el empleado con el sistema de información garantizando así que un empleado no pueda tener acceso a recursos que no debe y evitar que modifique elimine o dañe procesos a los cuales no debe tener acceso.

- En caso de acceso de un empleado se deberán realizar la actualización inmediata del perfil de seguridad ajustándolo al nuevo cargo.

- Asignar restricciones de acceso al centro de cómputo donde se encuentra el servidor principal, como también a todas las zonas donde el manejo de información sea crítico, además de las zonas donde se maneja el sistema eléctrico principal.

- Hacer control continuo y verificación del personal activo con el fin de evitar que existan fugas de seguridad por encontrarse activo perfiles de usuarios que ya no se encuentran vinculados con la empresa o que un perfil tenga mayores privilegios de los que deba tener.

- Manejo de contraseñas, cada usuario responderá por el acceso desde el perfil que le fue asignado, en caso de olvido de la contraseña debe solicitar su restablecimiento ante el administrador del sistema quien previa identificación positiva del empleado procederá a establecer una contraseña temporal la cual deberá ser cambiada inmediatamente al generar el acceso al sistema, con el fin de que solo el usuario cuente con la contraseña y así responsabilizarlo de su uso.

- Restricción del uso de internet, bloquear paginas no requerida para el funcionamiento de la empresa, entre ellas se destacan las redes sociales, servidores de música y video en línea, y correos electrónicos no pertenecientes al dominio de la empresa en este caso @celutel.com.co.

- Modificación y actualización de información: para realizar modificaciones y/o actualizaciones a la información ya registrada, se deberá solicitar por escrito ante el administrador de sistema para que este autorice y en caso de efectuarla generar un acta donde quede registrada la modificación y la justificación por la cual se llevó a cabo.

Política de Seguridad física, lógica y del entorno

Objetivo: mantener la protección de los equipos de cómputo de virus, optimizar el sistema de Backups, y garantizar el correcto uso del entorno del sistema de información

Aplicabilidad: esta política es aplicada a todo el personal, denomínese este administrativo, operativo y contratistas, en general se aplica a todo el personal que tenga contacto con el sistema de información de CELUTEL SAS

Directrices:

- Instalación y actualización de antivirus: adquisición de licencias de antivirus para todos los equipos con los que cuenta la empresa, y garantizar la actualización constante, programar escaneos de todos los equipos de cómputo mínimo una vez por semana, y con ello garantizar que el sistema esté libre de virus en todo momento.

- Crear perfiles de usuarios y contraseñas: se mantendrá así el acceso limitado a cada usuario asignando o denegándole permisos específicos a recursos y aplicativos dependiendo del rol que juegue este dentro de la empresa, en cuanto a las contraseñas estas deben ser de mínimo 8 caracteres en los que se debe incluir mínimo una letra en mayúscula y una en minúscula, números y un símbolo, además esta deberá ser cambiada cada 3 meses.

- Implementación del sistema de Backus de las bases de dato ubicadas en el servidor: este sistema se debe realizar de la siguiente forma; en primera instancia una copia diaria de la información se realizara a las 6:05 PM hora en la cual se suspenden las actividades de la empresa, esta copia se realizara en un disco extraíble, en él se almacenara la copia de seguridad que genere el administrador del sistema de ambas bases de datos, y en segunda instancia se programa una copia de seguridad semanal la cual

tendrá horario de 4:05 pm los días sábados al finalizar labores de la empresa, y de igual forma estará a cargo del administrador del sistema, con la única modificación de que esta será efectuada en un DVD el cual se rotulara con la fecha que corresponda; (ambos métodos dejaran el dispositivo almacenado en la caja fuerte de la empresa).

- Impedir instalación de aplicativos en los equipos de cómputo: establecer restricciones para que solo el personal capacitado y autorizado pueda realizar la instalación de aplicativos sobre los equipos de cómputo de la empresa.

- Bloquear puertos USB: ningún equipo podrá tener habilitado los puertos USB la información en la empresa siempre fluirá por la red, en caso de necesitar utilizar el puerto se debe solicitar por escrito ante el administrador del sistema quien otorgara por tiempo limitado el acceso al puerto o en su defecto el incluirá la información que traiga el medio de almacenamiento a la carpeta del empleado que lo solicite.

- Implementar capacitaciones de seguridad de entorno, dirigidas por los bomberos en las cuales se traten temas de primeros auxilios, manejo de rutas de evacuación y manejo de elementos extintores.

- Creación del sistema de soporte ininterrumpido de electricidad, establecer una UPS a cada equipo de cómputo con el fin de evitar dañas ocasionadas por las interrupciones del fluido eléctrico sin ser programado, esta UPS debe ser monitoreada para garantizar que la batería cumpla su función en caso de ser requerida

- Establecer condiciones para el manejo de equipos computacionales por personal externo a la empresa, que requieran conectarse a la red de datos.

- Proveer los recursos necesarios para proteger y mantener disponibles los controles en la empresa.

- El encargado de tecnología es el único autorizado para realizar cualquier cambio, asignación o traslado de recursos tecnológicos.

- Proveer herramientas tecnológicas para la seguridad de la información tales como antivirus, antimalware y antispyware (licenciados para garantizar la autenticidad del software).

Política de comunicaciones, dispositivos de red y servidor

Objetivo: garantizar el acceso a internet, y el buen funcionamiento de la red privada de CELUTEL SAS, como también mantener en óptimo funcionamiento el servidor principal y su motor de bases de datos.

Aplicabilidad: esta política es aplicada al personal administrativo y los encargados de la administración del centro de cómputo CELUTEL SAS

Directrices:

- Implementar sistema redundante de conexión a internet, preferiblemente con dos ISP distintos, con el fin de garantizar y darle continuidad al sistema en caso de que uno falle o presente denegación de servicios.

- Realizar mantenimiento preventivo y correctivo a el sistema cableado de red LAN, cada año.

- Limitar el ancho de banda en los puntos de acceso WIFI, realizar cambio de contraseña de la red una vez al mes.

- Realizar mantenimiento al servidor principal y a las bases de datos instaladas cada 6 meses.

ANEXO C.

TABLA DE DATOS PARA CÁLCULO DE IMAPACTO Y RIESGO

ACTIVO	AMENAZA	D	V	VA	D	I	P	RIESGO
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.24] Denegación de servicio	[D]	[10]	[10]	50%	[9]	33	{7,6}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.8] Difusión de software dañino	[D]	[10]	[10]	100%	[10]	3,6	{7,3}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.8] Difusión de software dañino	[I]	[10]	[10]	100%	[10]	3,6	{7,3}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.22] Manipulación de programas	[I]	[10]	[10]	100%	[10]	3,3	{7,3}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[E.25] Pérdida de equipos	[D]	[10]	[10]	100%	[10]	1,98	{7,1}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.27] Ocupación enemiga	[D]	[10]	[10]	100%	[10]	1,47	{7,0}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[I.6] Corte del suministro eléctrico	[D]	[10]	[10]	100%	[10]	1,05	{6,9}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[10]	[10]	100%	[10]	1,05	{6,9}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER	[N.1] Fuego	[D]	[10]	[10]	100%	[10]	1,05	{6,9}

(contable)								
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[I.1] Fuego	[D]	[10]	[10]	100%	[10]	1,05	{6,9}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[I.*] Desastres industriales	[D]	[10]	[10]	100%	[10]	1,05	{6,9}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[I.2] Daños por agua	[D]	[10]	[10]	100%	[10]	1,05	{6,9}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[N.2] Daños por agua	[D]	[10]	[10]	100%	[10]	1,05	{6,9}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.15] Modificación de la información	[I]	[10]	[10]	50%	[9]	3,6	{6,8}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.22] Manipulación de programas	[D]	[10]	[10]	50%	[9]	3,3	{6,8}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.25] Robo de equipos	[D]	[10]	[10]	100%	[10]	0,74	{6,7}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.5] Suplantación de la identidad	[A]	[9]	[9]	100%	[9]	3,6	{6,7}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.11] Acceso no autorizado	[A]	[9]	[9]	100%	[9]	3,6	{6,7}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[N.*] Desastres naturales	[D]	[10]	[10]	100%	[10]	0,52	{6,6}

[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[E.24] Caída del sistema por agotamiento de recursos	[D]	[10]	[10]	50%	[9]	1,98	{6,6}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[I.8] Fallo de servicios de comunicaciones	[D]	[10]	[10]	50%	[9]	1,05	{6,3}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[I.5] Avería de origen físico o lógico	[D]	[10]	[10]	50%	[9]	1,05	{6,3}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.23] Manipulación del hardware	[D]	[10]	[10]	50%	[9]	0,74	{6,2}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.26] Ataque destructivo	[D]	[10]	[10]	100%	[10]	0,147	{6,1}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.28] Indisponibilidad del personal	[D]	[10]	[10]	50%	[9]	0,67	{6,1}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.29] Extorsión	[I]	[10]	[10]	20%	[8]	2,3	{5,9}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.30] Ingeniería social (picaresca)	[I]	[10]	[10]	20%	[8]	1,26	{5,7}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[E.2] Errores del administrador del sistema / de la seguridad	[D]	[10]	[10]	20%	[8]	1,05	{5,6}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[E.2] Errores del administrador del sistema / de la seguridad	[I]	[10]	[10]	20%	[8]	1,05	{5,6}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER	[E.20] Vulnerabilidades de los programas (software)	[I]	[10]	[10]	20%	[8]	1,05	{5,6}

(contable)								
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.5] Suplantación de la identidad	[I]	[10]	[10]	10%	[7]	3,6	{5,6}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.11] Acceso no autorizado	[D]	[10]	[10]	10%	[7]	3,6	{5,6}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.11] Acceso no autorizado	[I]	[10]	[10]	10%	[7]	3,6	{5,6}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.18] Destrucción de la información	[D]	[10]	[10]	10%	[7]	3,6	{5,6}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.6] Abuso de privilegios de acceso	[D]	[10]	[10]	10%	[7]	3,3	{5,5}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.7] Uso no previsto	[D]	[10]	[10]	10%	[7]	3,3	{5,5}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.7] Uso no previsto	[I]	[10]	[10]	10%	[7]	3,3	{5,5}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.29] Extorsión	[D]	[10]	[10]	10%	[7]	2,3	{5,4}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D]	[10]	[10]	10%	[7]	1,98	{5,3}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER	[E.15] Alteración de la información	[I]	[10]	[10]	10%	[7]	1,98	{5,3}

(contable)								
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[E.8] Difusión de software dañino	[D]	[10]	[10]	10%	[7]	1,98	{5,3}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[E.8] Difusión de software dañino	[I]	[10]	[10]	10%	[7]	1,98	{5,3}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.10] Alteración de secuencia	[I]	[10]	[10]	10%	[7]	1,91	{5,3}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.30] Ingeniería social (picaresca)	[D]	[10]	[10]	10%	[7]	1,26	{5,2}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[E.28] Indisponibilidad del personal	[D]	[10]	[10]	10%	[7]	1,05	{5,1}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[I.3] Contaminación medioambiental	[D]	[10]	[10]	10%	[7]	1,05	{5,1}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[E.10] Errores de secuencia	[I]	[10]	[10]	10%	[7]	1,05	{5,1}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.8] Difusión de software dañino	[C]	[5]	[5]	100%	[5]	3,6	{4,4}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[E.21] Errores de mantenimiento / actualización de programas (software)	[D]	[10]	[10]	1%	[4]	19,8	{4,4}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER	[E.21] Errores de mantenimiento /	[I]	[10]	[10]	1%	[4]	19,8	{4,4}

(contable)	actualización de programas (software)							
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.22] Manipulación de programas	[C]	[5]	[5]	100%	[5]	3,3	{4,3}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[I.4] Contaminación electromagnética	[D]	[10]	[10]	10%	[7]	0,105	{4,2}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[E.25] Pérdida de equipos	[C]	[5]	[5]	100%	[5]	1,98	{4,2}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.19] Revelación de información	[C]	[5]	[5]	20%	[3]	36	{4,0}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.5] Suplantación de la identidad	[C]	[5]	[5]	50%	[4]	3,6	{3,9}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.11] Acceso no autorizado	[C]	[5]	[5]	50%	[4]	3,6	{3,9}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.25] Robo de equipos	[C]	[5]	[5]	100%	[5]	0,74	{3,8}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[E.18] Destrucción de la información	[D]	[10]	[10]	1%	[4]	1,98	{3,6}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[E.20] Vulnerabilidades de los programas (software)	[D]	[10]	[10]	1%	[4]	1,05	{3,3}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.23] Manipulación del hardware	[C]	[5]	[5]	50%	[4]	0,74	{3,2}

[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.29] Extorsión	[C]	[5]	[5]	20%	[3]	2,3	{3,0}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.30] Ingeniería social (picaresca)	[C]	[5]	[5]	20%	[3]	1,26	{2,7}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[E.2] Errores del administrador del sistema / de la seguridad	[C]	[5]	[5]	20%	[3]	1,05	{2,7}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[E.20] Vulnerabilidades de los programas (software)	[C]	[5]	[5]	20%	[3]	1,05	{2,7}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.7] Uso no previsto	[C]	[5]	[5]	10%	[2]	3,3	{2,6}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[E.19] Fugas de información	[C]	[5]	[5]	10%	[2]	1,98	{2,4}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[E.8] Difusión de software dañino	[C]	[5]	[5]	10%	[2]	1,98	{2,4}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.9] [Re-]encaminamiento de mensajes	[C]	[5]	[5]	10%	[2]	1,91	{2,4}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[E.9] Errores de [re-]encaminamiento	[C]	[5]	[5]	10%	[2]	1,05	{2,1}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[A.14] Interceptación de información (escucha)	[C]	[5]	[5]	5%	[1]	3,6	{2,1}
[01] [BD_GENERAL] Base Datos GENERAL LEDGER	[A.12] Análisis de tráfico	[C]	[5]	[5]	2%	[0]	1,91	{1,1}

(contable)								
[01] [BD_GENERAL] Base Datos GENERAL LEDGER (contable)	[I.11] Emanaciones electromagnéticas	[C]	[5]	[5]	1%	[0]	1,05	{0,87}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.24] Denegación de servicio	[D]	[9]	[9]	50%	[8]	33	{7,1}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.5] Suplantación de la identidad	[A]	[9]	[9]	100%	[9]	3,6	{6,7}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.11] Acceso no autorizado	[A]	[9]	[9]	100%	[9]	3,6	{6,7}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.8] Difusión de software dañino	[D]	[9]	[9]	100%	[9]	3,6	{6,7}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.8] Difusión de software dañino	[I]	[9]	[9]	100%	[9]	3,6	{6,7}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.22] Manipulación de programas	[I]	[9]	[9]	100%	[9]	3,3	{6,7}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.27] Ocupación enemiga	[D]	[9]	[9]	100%	[9]	1,47	{6,4}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[I.6] Corte del suministro eléctrico	[D]	[9]	[9]	100%	[9]	1,05	{6,3}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	[9]	100%	[9]	1,05	{6,3}

[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[I.1] Fuego	[D]	[9]	[9]	100%	[9]	1,05	{6,3}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[N.1] Fuego	[D]	[9]	[9]	100%	[9]	1,05	{6,3}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[I.*] Desastres industriales	[D]	[9]	[9]	100%	[9]	1,05	{6,3}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[I.2] Daños por agua	[D]	[9]	[9]	100%	[9]	1,05	{6,3}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[N.2] Daños por agua	[D]	[9]	[9]	100%	[9]	1,05	{6,3}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.15] Modificación de la información	[I]	[9]	[9]	50%	[8]	3,6	{6,2}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.22] Manipulación de programas	[D]	[9]	[9]	50%	[8]	3,3	{6,2}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[N.*] Desastres naturales	[D]	[9]	[9]	100%	[9]	0,52	{6,0}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.24] Caída del sistema por agotamiento de recursos	[D]	[9]	[9]	50%	[8]	1,98	{6,0}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[I.8] Fallo de servicios de comunicaciones	[D]	[9]	[9]	50%	[8]	1,05	{5,7}
[02] [BD_CELSIS] Base Datos CELUTEL (registro	[I.5] Avería de origen físico o lógico	[D]	[9]	[9]	50%	[8]	1,05	{5,7}

de clientes y ventas)								
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.23] Manipulación del hardware	[D]	[9]	[9]	50%	[8]	0,74	{5,6}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.28] Indisponibilidad del personal	[D]	[9]	[9]	50%	[8]	0,67	{5,6}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.26] Ataque destructivo	[D]	[9]	[9]	100%	[9]	0,147	{5,5}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.29] Extorsión	[I]	[9]	[9]	20%	[7]	2,3	{5,3}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.30] Ingeniería social (picaresca)	[I]	[9]	[9]	20%	[7]	1,26	{5,1}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.2] Errores del administrador del sistema / de la seguridad	[D]	[9]	[9]	20%	[7]	1,05	{5,0}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.2] Errores del administrador del sistema / de la seguridad	[I]	[9]	[9]	20%	[7]	1,05	{5,0}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.20] Vulnerabilidades de los programas (software)	[I]	[9]	[9]	20%	[7]	1,05	{5,0}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.5] Suplantación de la identidad	[I]	[9]	[9]	10%	[6]	3,6	{5,0}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.11] Acceso no autorizado	[D]	[9]	[9]	10%	[6]	3,6	{5,0}

[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.11] Acceso no autorizado	[I]	[9]	[9]	10%	[6]	3,6	{5,0}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.18] Destrucción de la información	[D]	[9]	[9]	10%	[6]	3,6	{5,0}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.6] Abuso de privilegios de acceso	[D]	[9]	[9]	10%	[6]	3,3	{4,9}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.7] Uso no previsto	[D]	[9]	[9]	10%	[6]	3,3	{4,9}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.7] Uso no previsto	[I]	[9]	[9]	10%	[6]	3,3	{4,9}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.29] Extorsión	[D]	[9]	[9]	10%	[6]	2,3	{4,8}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.25] Pérdida de equipos	[D]	[9]	[9]	5%	[5]	10	{4,8}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D]	[9]	[9]	10%	[6]	1,98	{4,7}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.15] Alteración de la información	[I]	[9]	[9]	10%	[6]	1,98	{4,7}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.8] Difusión de software dañino	[D]	[9]	[9]	10%	[6]	1,98	{4,7}

[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.8] Difusión de software dañino	[I]	[9]	[9]	10%	[6]	1,98	{4,7}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.10] Alteración de secuencia	[I]	[9]	[9]	10%	[6]	1,91	{4,7}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.25] Robo de equipos	[D]	[9]	[9]	5%	[5]	7,4	{4,7}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.30] Ingeniería social (picaresca)	[D]	[9]	[9]	10%	[6]	1,26	{4,6}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.28] Indisponibilidad del personal	[D]	[9]	[9]	10%	[6]	1,05	{4,5}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[I.3] Contaminación medioambiental	[D]	[9]	[9]	10%	[6]	1,05	{4,5}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.10] Errores de secuencia	[I]	[9]	[9]	10%	[6]	1,05	{4,5}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.21] Errores de mantenimiento / actualización de programas (software)	[D]	[9]	[9]	1%	[3]	19,8	{3,9}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.21] Errores de mantenimiento / actualización de programas (software)	[I]	[9]	[9]	1%	[3]	19,8	{3,9}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[I.4] Contaminación electromagnética	[D]	[9]	[9]	10%	[6]	0,105	{3,6}

[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.8] Difusión de software dañino	[C]	[3]	[3]	100%	[3]	3,6	{3,2}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.22] Manipulación de programas	[C]	[3]	[3]	100%	[3]	3,3	{3,2}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.18] Destrucción de la información	[D]	[9]	[9]	1%	[3]	1,98	{3,0}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.19] Revelación de información	[C]	[3]	[3]	20%	[1]	36	{2,9}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.20] Vulnerabilidades de los programas (software)	[D]	[9]	[9]	1%	[3]	1,05	{2,7}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.5] Suplantación de la identidad	[C]	[3]	[3]	50%	[2]	3,6	{2,7}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.11] Acceso no autorizado	[C]	[3]	[3]	50%	[2]	3,6	{2,7}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.23] Manipulación del hardware	[C]	[3]	[3]	50%	[2]	0,74	{2,1}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.29] Extorsión	[C]	[3]	[3]	20%	[1]	2,3	{1,8}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.25] Pérdida de equipos	[C]	[3]	[3]	10%	[0]	10	{1,8}
[02] [BD_CELSIS] Base Datos CELUTEL (registro	[A.25] Robo de equipos	[C]	[3]	[3]	10%	[0]	7,4	{1,7}

de clientes y ventas)								
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.30] Ingeniería social (picaresca)	[C]	[3]	[3]	20%	[1]	1,26	{1,6}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.2] Errores del administrador del sistema / de la seguridad	[C]	[3]	[3]	20%	[1]	1,05	{1,5}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.20] Vulnerabilidades de los programas (software)	[C]	[3]	[3]	20%	[1]	1,05	{1,5}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.7] Uso no previsto	[C]	[3]	[3]	10%	[0]	3,3	{1,4}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.19] Fugas de información	[C]	[3]	[3]	10%	[0]	1,98	{1,2}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.8] Difusión de software dañino	[C]	[3]	[3]	10%	[0]	1,98	{1,2}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.9] [Re-]encaminamiento de mensajes	[C]	[3]	[3]	10%	[0]	1,91	{1,2}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[E.9] Errores de [re-]encaminamiento	[C]	[3]	[3]	10%	[0]	1,05	{0,99}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.14] Interceptación de información (escucha)	[C]	[3]	[3]	5%	[0]	3,6	{0,98}
[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[A.12] Análisis de tráfico	[C]	[3]	[3]	2%	[0]	1,91	{0,79}

[02] [BD_CELSIS] Base Datos CELUTEL (registro de clientes y ventas)	[I.11] Emanaciones electromagnéticas	[C]	[3]	[3]	1%	[0]	1,05	{0,64}
[001] [EMAIL] correo electrónico	[A.24] Denegación de servicio	[D]	[2]	[2]	50%	[1]	33	{2,9}
[001] [EMAIL] correo electrónico	[E.24] Caída del sistema por agotamiento de recursos	[D]	[2]	[2]	50%	[1]	19,8	{2,7}
[001] [EMAIL] correo electrónico	[A.28] Indisponibilidad del personal	[D]	[2]	[2]	50%	[1]	0,67	{1,4}
[001] [EMAIL] correo electrónico	[E.2] Errores del administrador del sistema / de la seguridad	[D]	[2]	[2]	20%	[0]	1,05	{0,98}
[001] [EMAIL] correo electrónico	[A.18] Destrucción de la información	[D]	[2]	[2]	10%	[0]	3,6	{0,97}
[001] [EMAIL] correo electrónico	[A.29] Extorsión	[D]	[2]	[2]	10%	[0]	2,3	{0,93}
[001] [EMAIL] correo electrónico	[E.1] Errores de los usuarios	[D]	[2]	[2]	10%	[0]	1,98	{0,92}
[001] [EMAIL] correo electrónico	[A.30] Ingeniería social (picaresca)	[D]	[2]	[2]	10%	[0]	1,26	{0,89}
[001] [EMAIL] correo electrónico	[E.28] Indisponibilidad del personal	[D]	[2]	[2]	10%	[0]	1,05	{0,87}
[001] [EMAIL] correo electrónico	[A.6] Abuso de privilegios de acceso	[D]	[2]	[2]	1%	[0]	3,3	{0,61}
[001] [EMAIL] correo electrónico	[A.7] Uso no previsto	[D]	[2]	[2]	1%	[0]	3,3	{0,61}
[001] [EMAIL] correo electrónico	[E.18] Destrucción de la información	[D]	[2]	[2]	1%	[0]	1,98	{0,57}
[002] [S_INTERNET] Servicio de conexión a	[I.8] Fallo de servicios de comunicaciones	[D]	[9]	[9]	100%	[9]	1,05	{6,3}

internet								
[002] [S_INTERNET] Servicio de conexión a internet	[A.18] Destrucción de la información	[D]	[9]	[9]	50%	[8]	3,6	{6,2}
[002] [S_INTERNET] Servicio de conexión a internet	[A.24] Denegación de servicio	[D]	[9]	[9]	50%	[8]	3,3	{6,2}
[002] [S_INTERNET] Servicio de conexión a internet	[E.18] Destrucción de la información	[D]	[9]	[9]	10%	[6]	1,98	{4,7}
[010] [PC_S] servidor principal	[A.3] Manipulación de los registros de actividad (log)	[I]	[10]	[10]	50%	[9]	147	{8,2}
[010] [PC_S] servidor principal	[A.24] Denegación de servicio	[D]	[10]	[10]	100%	[10]	6,6	{7,6}
[010] [PC_S] servidor principal	[A.5] Suplantación de la identidad	[A]	[9]	[9]	100%	[9]	36	{7,6}
[010] [PC_S] servidor principal	[E.24] Caída del sistema por agotamiento de recursos	[D]	[10]	[10]	50%	[9]	19,8	{7,4}
[010] [PC_S] servidor principal	[A.8] Difusión de software dañino	[D]	[10]	[10]	100%	[10]	3,6	{7,3}
[010] [PC_S] servidor principal	[A.8] Difusión de software dañino	[I]	[10]	[10]	100%	[10]	3,6	{7,3}
[010] [PC_S] servidor principal	[A.22] Manipulación de programas	[I]	[10]	[10]	100%	[10]	3,3	{7,3}
[010] [PC_S] servidor principal	[E.25] Pérdida de equipos	[D]	[10]	[10]	100%	[10]	1,98	{7,1}
[010] [PC_S] servidor principal	[A.5] Suplantación de la identidad	[C]	[9]	[9]	50%	[8]	36	{7,1}
[010] [PC_S] servidor principal	[A.6] Abuso de privilegios de acceso	[C]	[9]	[9]	50%	[8]	33	{7,1}

[010] [PC_S] servidor principal	[A.26] Ataque destructivo	[D]	[10]	[10]	100%	[10]	1,47	{7,0}
[010] [PC_S] servidor principal	[I.6] Corte del suministro eléctrico	[D]	[10]	[10]	100%	[10]	1,05	{6,9}
[010] [PC_S] servidor principal	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[10]	[10]	100%	[10]	1,05	{6,9}
[010] [PC_S] servidor principal	[A.22] Manipulación de programas	[D]	[10]	[10]	50%	[9]	3,3	{6,8}
[010] [PC_S] servidor principal	[A.25] Robo de equipos	[D]	[10]	[10]	100%	[10]	0,74	{6,7}
[010] [PC_S] servidor principal	[A.8] Difusión de software dañino	[C]	[9]	[9]	100%	[9]	3,6	{6,7}
[010] [PC_S] servidor principal	[A.22] Manipulación de programas	[C]	[9]	[9]	100%	[9]	3,3	{6,7}
[010] [PC_S] servidor principal	[I.1] Fuego	[D]	[10]	[10]	100%	[10]	0,52	{6,6}
[010] [PC_S] servidor principal	[I.*] Desastres industriales	[D]	[10]	[10]	100%	[10]	0,52	{6,6}
[010] [PC_S] servidor principal	[E.25] Pérdida de equipos	[C]	[9]	[9]	100%	[9]	1,98	{6,5}
[010] [PC_S] servidor principal	[A.5] Suplantación de la identidad	[I]	[10]	[10]	10%	[7]	36	{6,4}
[010] [PC_S] servidor principal	[A.6] Abuso de privilegios de acceso	[I]	[10]	[10]	10%	[7]	33	{6,4}
[010] [PC_S] servidor principal	[I.5] Avería de origen físico o lógico	[D]	[10]	[10]	50%	[9]	1,05	{6,3}
[010] [PC_S] servidor principal	[A.23] Manipulación del hardware	[D]	[10]	[10]	50%	[9]	0,74	{6,2}
[010] [PC_S] servidor principal	[A.11] Acceso no autorizado	[C]	[9]	[9]	50%	[8]	3,6	{6,2}

[010] [PC_S] servidor principal	[I.2] Daños por agua	[D]	[10]	[10]	50%	[9]	0,52	{6,1}
[010] [PC_S] servidor principal	[A.25] Robo de equipos	[C]	[9]	[9]	100%	[9]	0,74	{6,1}
[010] [PC_S] servidor principal	[N.1] Fuego	[D]	[10]	[10]	100%	[10]	0,105	{6,0}
[010] [PC_S] servidor principal	[N.*] Desastres naturales	[D]	[10]	[10]	100%	[10]	0,105	{6,0}
[010] [PC_S] servidor principal	[A.23] Manipulación del hardware	[C]	[9]	[9]	50%	[8]	0,74	{5,6}
[010] [PC_S] servidor principal	[E.20] Vulnerabilidades de los programas (software)	[I]	[10]	[10]	20%	[8]	1,05	{5,6}
[010] [PC_S] servidor principal	[A.11] Acceso no autorizado	[D]	[10]	[10]	10%	[7]	3,6	{5,6}
[010] [PC_S] servidor principal	[A.11] Acceso no autorizado	[I]	[10]	[10]	10%	[7]	3,6	{5,6}
[010] [PC_S] servidor principal	[N.2] Daños por agua	[D]	[10]	[10]	50%	[9]	0,105	{5,4}
[010] [PC_S] servidor principal	[I.3] Contaminación medioambiental	[D]	[10]	[10]	50%	[9]	0,105	{5,4}
[010] [PC_S] servidor principal	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D]	[10]	[10]	10%	[7]	1,98	{5,3}
[010] [PC_S] servidor principal	[E.8] Difusión de software dañino	[D]	[10]	[10]	10%	[7]	1,98	{5,3}
[010] [PC_S] servidor principal	[E.8] Difusión de software dañino	[I]	[10]	[10]	10%	[7]	1,98	{5,3}
[010] [PC_S] servidor principal	[I.4] Contaminación electromagnética	[D]	[10]	[10]	10%	[7]	1,05	{5,1}
[010] [PC_S] servidor	[E.20] Vulnerabilidades de	[C]	[9]	[9]	20%	[7]	1,05	{5,0}

principal	los programas (software)							
[010] [PC_S] servidor principal	[A.7] Uso no previsto	[C]	[9]	[9]	10%	[6]	3,3	{4,9}
[010] [PC_S] servidor principal	[E.8] Difusión de software dañino	[C]	[9]	[9]	10%	[6]	1,98	{4,7}
[010] [PC_S] servidor principal	[A.6] Abuso de privilegios de acceso	[D]	[10]	[10]	1%	[4]	33	{4,6}
[010] [PC_S] servidor principal	[E.21] Errores de mantenimiento / actualización de programas (software)	[D]	[10]	[10]	1%	[4]	19,8	{4,4}
[010] [PC_S] servidor principal	[E.21] Errores de mantenimiento / actualización de programas (software)	[I]	[10]	[10]	1%	[4]	19,8	{4,4}
[010] [PC_S] servidor principal	[A.7] Uso no previsto	[D]	[10]	[10]	1%	[4]	3,3	{3,8}
[010] [PC_S] servidor principal	[A.7] Uso no previsto	[I]	[10]	[10]	1%	[4]	3,3	{3,8}
[010] [PC_S] servidor principal	[E.18] Destrucción de la información	[D]	[10]	[10]	1%	[4]	1,98	{3,6}
[010] [PC_S] servidor principal	[E.15] Alteración de la información	[I]	[10]	[10]	1%	[4]	1,98	{3,6}
[010] [PC_S] servidor principal	[E.20] Vulnerabilidades de los programas (software)	[D]	[10]	[10]	1%	[4]	1,05	{3,3}
[010] [PC_S] servidor principal	[E.3] Errores de monitorización (log)	[I]	[10]	[10]	1%	[4]	1,05	{3,3}
[010] [PC_S] servidor principal	[I.11] Emanaciones electromagnéticas	[C]	[9]	[9]	1%	[3]	1,05	{2,7}
[011] [PC] Computadora	[A.15] Modificación de la información	[I]	[3]	[3]	100%	[3]	18	{3,8}

[011] [PC] Computadora	[A.8] Difusión de software dañino	[I]	[3]	[3]	100%	[3]	3,6	{3,2}
[011] [PC] Computadora	[A.22] Manipulación de programas	[I]	[3]	[3]	100%	[3]	3,3	{3,2}
[011] [PC] Computadora	[A.24] Denegación de servicio	[D]	[5]	[5]	10%	[2]	6,6	{2,8}
[011] [PC] Computadora	[E.24] Caída del sistema por agotamiento de recursos	[D]	[5]	[5]	5%	[1]	19,8	{2,7}
[011] [PC] Computadora	[A.18] Destrucción de la información	[D]	[5]	[5]	10%	[2]	3,6	{2,6}
[011] [PC] Computadora	[A.8] Difusión de software dañino	[D]	[5]	[5]	10%	[2]	3,6	{2,6}
[011] [PC] Computadora	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D]	[5]	[5]	10%	[2]	1,98	{2,4}
[011] [PC] Computadora	[E.18] Destrucción de la información	[D]	[5]	[5]	10%	[2]	1,98	{2,4}
[011] [PC] Computadora	[I.10] Degradación de los soportes de almacenamiento de la información	[D]	[5]	[5]	10%	[2]	1,05	{2,1}
[011] [PC] Computadora	[I.6] Corte del suministro eléctrico	[D]	[5]	[5]	10%	[2]	1,05	{2,1}
[011] [PC] Computadora	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[5]	[5]	10%	[2]	1,05	{2,1}
[011] [PC] Computadora	[A.22] Manipulación de programas	[D]	[5]	[5]	5%	[1]	3,3	{2,1}
[011] [PC] Computadora	[I.*] Desastres industriales	[D]	[5]	[5]	10%	[2]	0,52	{1,9}

[011] [PC] Computadora	[I.1] Fuego	[D]	[5]	[5]	10%	[2]	0,52	{1,9}
[011] [PC] Computadora	[I.3] Contaminación medioambiental	[D]	[5]	[5]	5%	[1]	1,05	{1,6}
[011] [PC] Computadora	[I.5] Avería de origen físico o lógico	[D]	[5]	[5]	5%	[1]	1,05	{1,6}
[011] [PC] Computadora	[E.20] Vulnerabilidades de los programas (software)	[I]	[3]	[3]	20%	[1]	1,05	{1,5}
[011] [PC] Computadora	[N.*] Desastres naturales	[D]	[5]	[5]	10%	[2]	0,105	{1,3}
[011] [PC] Computadora	[N.1] Fuego	[D]	[5]	[5]	10%	[2]	0,105	{1,3}
[011] [PC] Computadora	[I.2] Daños por agua	[D]	[5]	[5]	5%	[1]	0,52	{1,3}
[011] [PC] Computadora	[E.8] Difusión de software dañino	[I]	[3]	[3]	10%	[0]	1,98	{1,2}
[011] [PC] Computadora	[A.23] Manipulación del hardware	[D]	[5]	[5]	5%	[1]	0,147	{0,97}
[011] [PC] Computadora	[A.11] Acceso no autorizado	[D]	[5]	[5]	1%	[0]	3,6	{0,97}
[011] [PC] Computadora	[N.2] Daños por agua	[D]	[5]	[5]	5%	[1]	0,105	{0,94}
[011] [PC] Computadora	[E.1] Errores de los usuarios	[I]	[3]	[3]	5%	[0]	1,98	{0,93}
[011] [PC] Computadora	[E.25] Pérdida de equipos	[D]	[5]	[5]	1%	[0]	1,98	{0,92}
[011] [PC] Computadora	[E.8] Difusión de software dañino	[D]	[5]	[5]	1%	[0]	1,98	{0,92}
[011] [PC] Computadora	[A.26] Ataque destructivo	[D]	[5]	[5]	1%	[0]	1,47	{0,90}
[011] [PC] Computadora	[A.25] Robo de equipos	[D]	[5]	[5]	1%	[0]	1,47	{0,90}
[011] [PC] Computadora	[I.4] Contaminación electromagnética	[D]	[5]	[5]	1%	[0]	1,05	{0,87}
[011] [PC] Computadora	[E.21] Errores de mantenimiento / actualización de programas (software)	[I]	[3]	[3]	1%	[0]	19,8	{0,86}

[011] [PC] Computadora	[A.11] Acceso no autorizado	[I]	[3]	[3]	1%	[0]	3,6	{0,73}
[011] [PC] Computadora	[A.7] Uso no previsto	[I]	[3]	[3]	1%	[0]	3,3	{0,72}
[011] [PC] Computadora	[E.15] Alteración de la información	[I]	[3]	[3]	1%	[0]	1,98	{0,68}
[011] [PC] Computadora	[E.21] Errores de mantenimiento / actualización de programas (software)	[D]	[5]	[5]	0	[0]	19,8	{0}
[011] [PC] Computadora	[A.15] Modificación de la información	[D]	[5]	[5]	0	[0]	18	{0}
[011] [PC] Computadora	[A.7] Uso no previsto	[D]	[5]	[5]	0	[0]	3,3	{0}
[011] [PC] Computadora	[E.1] Errores de los usuarios	[D]	[5]	[5]	0	[0]	1,98	{0}
[011] [PC] Computadora	[E.15] Alteración de la información	[D]	[5]	[5]	0	[0]	1,98	{0}
[011] [PC] Computadora	[E.20] Vulnerabilidades de los programas (software)	[D]	[5]	[5]	0	[0]	1,05	{0}
[012] [PRINT] medios de impresión	[A.24] Denegación de servicio	[D]	[5]	[5]	100%	[5]	6,6	{4,6}
[012] [PRINT] medios de impresión	[E.24] Caída del sistema por agotamiento de recursos	[D]	[5]	[5]	50%	[4]	19,8	{4,5}
[012] [PRINT] medios de impresión	[E.25] Pérdida de equipos	[D]	[5]	[5]	100%	[5]	1,98	{4,2}
[012] [PRINT] medios de impresión	[A.26] Ataque destructivo	[D]	[5]	[5]	100%	[5]	1,47	{4,0}
[012] [PRINT] medios de impresión	[I.6] Corte del suministro eléctrico	[D]	[5]	[5]	100%	[5]	1,05	{3,9}
[012] [PRINT] medios de impresión	[I.7] Condiciones inadecuadas de	[D]	[5]	[5]	100%	[5]	1,05	{3,9}

	temperatura o humedad							
[012] [PRINT] medios de impresión	[A.25] Robo de equipos	[D]	[5]	[5]	100%	[5]	0,74	{3,8}
[012] [PRINT] medios de impresión	[I.*] Desastres industriales	[D]	[5]	[5]	100%	[5]	0,52	{3,6}
[012] [PRINT] medios de impresión	[I.1] Fuego	[D]	[5]	[5]	100%	[5]	0,52	{3,6}
[012] [PRINT] medios de impresión	[I.5] Avería de origen físico o lógico	[D]	[5]	[5]	50%	[4]	1,05	{3,4}
[012] [PRINT] medios de impresión	[A.23] Manipulación del hardware	[D]	[5]	[5]	50%	[4]	0,74	{3,2}
[012] [PRINT] medios de impresión	[I.2] Daños por agua	[D]	[5]	[5]	50%	[4]	0,52	{3,1}
[012] [PRINT] medios de impresión	[N.1] Fuego	[D]	[5]	[5]	100%	[5]	0,105	{3,0}
[012] [PRINT] medios de impresión	[N.*] Desastres naturales	[D]	[5]	[5]	100%	[5]	0,105	{3,0}
[012] [PRINT] medios de impresión	[A.11] Acceso no autorizado	[D]	[5]	[5]	10%	[2]	3,6	{2,6}
[012] [PRINT] medios de impresión	[N.2] Daños por agua	[D]	[5]	[5]	50%	[4]	0,105	{2,5}
[012] [PRINT] medios de impresión	[I.3] Contaminación medioambiental	[D]	[5]	[5]	50%	[4]	0,105	{2,5}
[012] [PRINT] medios de impresión	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D]	[5]	[5]	10%	[2]	1,98	{2,4}
[012] [PRINT] medios de impresión	[I.4] Contaminación electromagnética	[D]	[5]	[5]	10%	[2]	1,05	{2,1}
[013] [SCAN] escáneres	[A.24] Denegación de servicio	[D]	[1]	[1]	100%	[1]	6,6	{2,3}

[013] [SCAN] escáneres	[E.24] Caída del sistema por agotamiento de recursos	[D]	[1]	[1]	50%	[0]	19,8	{2,2}
[013] [SCAN] escáneres	[E.25] Pérdida de equipos	[D]	[1]	[1]	100%	[1]	1,98	{1,8}
[013] [SCAN] escáneres	[A.26] Ataque destructivo	[D]	[1]	[1]	100%	[1]	1,47	{1,7}
[013] [SCAN] escáneres	[I.6] Corte del suministro eléctrico	[D]	[1]	[1]	100%	[1]	1,05	{1,6}
[013] [SCAN] escáneres	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[1]	[1]	100%	[1]	1,05	{1,6}
[013] [SCAN] escáneres	[A.25] Robo de equipos	[D]	[1]	[1]	100%	[1]	0,74	{1,4}
[013] [SCAN] escáneres	[I.*] Desastres industriales	[D]	[1]	[1]	100%	[1]	0,52	{1,3}
[013] [SCAN] escáneres	[I.1] Fuego	[D]	[1]	[1]	100%	[1]	0,52	{1,3}
[013] [SCAN] escáneres	[I.5] Avería de origen físico o lógico	[D]	[1]	[1]	50%	[0]	1,05	{1,0}
[013] [SCAN] escáneres	[A.23] Manipulación del hardware	[D]	[1]	[1]	50%	[0]	0,74	{0,97}
[013] [SCAN] escáneres	[I.2] Daños por agua	[D]	[1]	[1]	50%	[0]	0,52	{0,95}
[013] [SCAN] escáneres	[N.1] Fuego	[D]	[1]	[1]	100%	[1]	0,105	{0,93}
[013] [SCAN] escáneres	[N.*] Desastres naturales	[D]	[1]	[1]	100%	[1]	0,105	{0,93}
[013] [SCAN] escáneres	[A.11] Acceso no autorizado	[D]	[1]	[1]	10%	[0]	3,6	{0,85}
[013] [SCAN] escáneres	[I.3] Contaminación medioambiental	[D]	[1]	[1]	50%	[0]	0,105	{0,82}
[013] [SCAN] escáneres	[N.2] Daños por agua	[D]	[1]	[1]	50%	[0]	0,105	{0,82}
[013] [SCAN] escáneres	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D]	[1]	[1]	10%	[0]	1,98	{0,80}
[013] [SCAN] escáneres	[I.4] Contaminación	[D]	[1]	[1]	10%	[0]	1,05	{0,75}

	electromagnética							
[014] [SWITCH] concentrador red local	[A.24] Denegación de servicio	[D]	[9]	[9]	100%	[9]	6,6	{7,0}
[014] [SWITCH] concentrador red local	[E.24] Caída del sistema por agotamiento de recursos	[D]	[9]	[9]	50%	[8]	19,8	{6,9}
[014] [SWITCH] concentrador red local	[A.26] Ataque destructivo	[D]	[9]	[9]	100%	[9]	1,47	{6,4}
[014] [SWITCH] concentrador red local	[I.6] Corte del suministro eléctrico	[D]	[9]	[9]	100%	[9]	1,05	{6,3}
[014] [SWITCH] concentrador red local	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	[9]	100%	[9]	1,05	{6,3}
[014] [SWITCH] concentrador red local	[A.23] Manipulación del hardware	[D]	[9]	[9]	100%	[9]	0,74	{6,1}
[014] [SWITCH] concentrador red local	[I.*] Desastres industriales	[D]	[9]	[9]	100%	[9]	0,52	{6,0}
[014] [SWITCH] concentrador red local	[I.1] Fuego	[D]	[9]	[9]	100%	[9]	0,52	{6,0}
[014] [SWITCH] concentrador red local	[I.5] Avería de origen físico o lógico	[D]	[9]	[9]	50%	[8]	1,05	{5,7}
[014] [SWITCH] concentrador red local	[I.2] Daños por agua	[D]	[9]	[9]	50%	[8]	0,52	{5,5}
[014] [SWITCH] concentrador red local	[N.*] Desastres naturales	[D]	[9]	[9]	100%	[9]	0,105	{5,4}
[014] [SWITCH] concentrador red local	[N.1] Fuego	[D]	[9]	[9]	100%	[9]	0,105	{5,4}
[014] [SWITCH] concentrador red local	[E.25] Pérdida de equipos	[D]	[9]	[9]	20%	[7]	1,98	{5,3}
[014] [SWITCH] concentrador red local	[A.11] Acceso no autorizado	[D]	[9]	[9]	10%	[6]	3,6	{5,0}

[014] [SWITCH] concentrador red local	[I.3] Contaminación medioambiental	[D]	[9]	[9]	50%	[8]	0,105	{4,9}
[014] [SWITCH] concentrador red local	[N.2] Daños por agua	[D]	[9]	[9]	50%	[8]	0,105	{4,9}
[014] [SWITCH] concentrador red local	[A.25] Robo de equipos	[D]	[9]	[9]	20%	[7]	0,74	{4,9}
[014] [SWITCH] concentrador red local	[A.7] Uso no previsto	[D]	[9]	[9]	10%	[6]	3,3	{4,9}
[014] [SWITCH] concentrador red local	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D]	[9]	[9]	10%	[6]	1,98	{4,7}
[014] [SWITCH] concentrador red local	[I.4] Contaminación electromagnética	[D]	[9]	[9]	10%	[6]	1,05	{4,5}
[015] [CONMUTADOR] conmutador interno telefónico	[A.24] Denegación de servicio	[D]	[1]	[1]	100%	[1]	6,6	{2,3}
[015] [CONMUTADOR] conmutador interno telefónico	[E.24] Caída del sistema por agotamiento de recursos	[D]	[1]	[1]	50%	[0]	19,8	{2,2}
[015] [CONMUTADOR] conmutador interno telefónico	[E.25] Pérdida de equipos	[D]	[1]	[1]	100%	[1]	1,98	{1,8}
[015] [CONMUTADOR] conmutador interno telefónico	[A.26] Ataque destructivo	[D]	[1]	[1]	100%	[1]	1,47	{1,7}
[015] [CONMUTADOR] conmutador interno telefónico	[I.6] Corte del suministro eléctrico	[D]	[1]	[1]	100%	[1]	1,05	{1,6}
[015] [CONMUTADOR] conmutador interno telefónico	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[1]	[1]	100%	[1]	1,05	{1,6}

[015] [CONMUTADOR] conmutador interno telefónico	[A.25] Robo de equipos	[D]	[1]	[1]	100%	[1]	0,74	{1,4}
[015] [CONMUTADOR] conmutador interno telefónico	[I.*] Desastres industriales	[D]	[1]	[1]	100%	[1]	0,52	{1,3}
[015] [CONMUTADOR] conmutador interno telefónico	[I.1] Fuego	[D]	[1]	[1]	100%	[1]	0,52	{1,3}
[015] [CONMUTADOR] conmutador interno telefónico	[I.5] Avería de origen físico o lógico	[D]	[1]	[1]	50%	[0]	1,05	{1,0}
[015] [CONMUTADOR] conmutador interno telefónico	[A.23] Manipulación del hardware	[D]	[1]	[1]	50%	[0]	0,74	{0,97}
[015] [CONMUTADOR] conmutador interno telefónico	[I.2] Daños por agua	[D]	[1]	[1]	50%	[0]	0,52	{0,95}
[015] [CONMUTADOR] conmutador interno telefónico	[N.1] Fuego	[D]	[1]	[1]	100%	[1]	0,105	{0,93}
[015] [CONMUTADOR] conmutador interno telefónico	[N.*] Desastres naturales	[D]	[1]	[1]	100%	[1]	0,105	{0,93}
[015] [CONMUTADOR] conmutador interno telefónico	[A.11] Acceso no autorizado	[D]	[1]	[1]	10%	[0]	3,6	{0,85}
[015] [CONMUTADOR] conmutador interno telefónico	[I.3] Contaminación medioambiental	[D]	[1]	[1]	50%	[0]	0,105	{0,82}
[015] [CONMUTADOR] conmutador interno	[N.2] Daños por agua	[D]	[1]	[1]	50%	[0]	0,105	{0,82}

telefónico								
[015] [CONMUTADOR] conmutador interno telefónico	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D]	[1]	[1]	10%	[0]	1,98	{0,80}
[015] [CONMUTADOR] conmutador interno telefónico	[I.4] Contaminación electromagnética	[D]	[1]	[1]	10%	[0]	1,05	{0,75}
[016] [CÁMARA] cámaras de seguridad	[A.24] Denegación de servicio	[D]	[1]	[1]	100%	[1]	6,6	{2,3}
[016] [CÁMARA] cámaras de seguridad	[E.24] Caída del sistema por agotamiento de recursos	[D]	[1]	[1]	50%	[0]	19,8	{2,2}
[016] [CÁMARA] cámaras de seguridad	[E.25] Pérdida de equipos	[D]	[1]	[1]	100%	[1]	1,98	{1,8}
[016] [CÁMARA] cámaras de seguridad	[A.26] Ataque destructivo	[D]	[1]	[1]	100%	[1]	1,47	{1,7}
[016] [CÁMARA] cámaras de seguridad	[I.6] Corte del suministro eléctrico	[D]	[1]	[1]	100%	[1]	1,05	{1,6}
[016] [CÁMARA] cámaras de seguridad	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[1]	[1]	100%	[1]	1,05	{1,6}
[016] [CÁMARA] cámaras de seguridad	[A.25] Robo de equipos	[D]	[1]	[1]	100%	[1]	0,74	{1,4}
[016] [CÁMARA] cámaras de seguridad	[I.1] Fuego	[D]	[1]	[1]	100%	[1]	0,52	{1,3}
[016] [CÁMARA] cámaras de seguridad	[I.*] Desastres industriales	[D]	[1]	[1]	100%	[1]	0,52	{1,3}
[016] [CÁMARA] cámaras de seguridad	[I.5] Avería de origen físico o lógico	[D]	[1]	[1]	50%	[0]	1,05	{1,0}
[016] [CÁMARA] cámaras	[A.23] Manipulación del	[D]	[1]	[1]	50%	[0]	0,74	{0,97}

de seguridad	hardware							
[016] [CÁMARA] cámaras de seguridad	[I.2] Daños por agua	[D]	[1]	[1]	50%	[0]	0,52	{0,95}
[016] [CÁMARA] cámaras de seguridad	[N.1] Fuego	[D]	[1]	[1]	100%	[1]	0,105	{0,93}
[016] [CÁMARA] cámaras de seguridad	[N.*] Desastres naturales	[D]	[1]	[1]	100%	[1]	0,105	{0,93}
[016] [CÁMARA] cámaras de seguridad	[A.11] Acceso no autorizado	[D]	[1]	[1]	10%	[0]	3,6	{0,85}
[016] [CÁMARA] cámaras de seguridad	[N.2] Daños por agua	[D]	[1]	[1]	50%	[0]	0,105	{0,82}
[016] [CÁMARA] cámaras de seguridad	[I.3] Contaminación medioambiental	[D]	[1]	[1]	50%	[0]	0,105	{0,82}
[016] [CÁMARA] cámaras de seguridad	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D]	[1]	[1]	10%	[0]	1,98	{0,80}
[016] [CÁMARA] cámaras de seguridad	[I.4] Contaminación electromagnética	[D]	[1]	[1]	10%	[0]	1,05	{0,75}
[017] [ADSL] Conexión a internet brindada por un ISP	[A.24] Denegación de servicio	[D]	[10]	[10]	50%	[9]	33	{7,6}
[017] [ADSL] Conexión a internet brindada por un ISP	[A.18] Destrucción de la información	[D]	[10]	[10]	50%	[9]	3,6	{6,8}
[017] [ADSL] Conexión a internet brindada por un ISP	[E.24] Caída del sistema por agotamiento de recursos	[D]	[10]	[10]	50%	[9]	1,98	{6,6}
[017] [ADSL] Conexión a internet brindada por un ISP	[I.8] Fallo de servicios de comunicaciones	[D]	[10]	[10]	50%	[9]	1,05	{6,3}

[017] [ADSL] Conexión a internet brindada por un ISP	[E.2] Errores del administrador del sistema / de la seguridad	[D]	[10]	[10]	20%	[8]	1,05	{5,6}
[017] [ADSL] Conexión a internet brindada por un ISP	[A.7] Uso no previsto	[D]	[10]	[10]	10%	[7]	3,3	{5,5}
[018] [TEL] red telefónica	[A.24] Denegación de servicio	[D]	[5]	[5]	50%	[4]	33	{4,7}
[018] [TEL] red telefónica	[A.18] Destrucción de la información	[D]	[5]	[5]	50%	[4]	3,6	{3,9}
[018] [TEL] red telefónica	[E.24] Caída del sistema por agotamiento de recursos	[D]	[5]	[5]	50%	[4]	1,98	{3,6}
[018] [TEL] red telefónica	[I.8] Fallo de servicios de comunicaciones	[D]	[5]	[5]	50%	[4]	1,05	{3,4}
[018] [TEL] red telefónica	[E.2] Errores del administrador del sistema / de la seguridad	[D]	[5]	[5]	20%	[3]	1,05	{2,7}
[018] [TEL] red telefónica	[A.7] Uso no previsto	[D]	[5]	[5]	10%	[2]	3,3	{2,6}
[019] [LAN] red local	[A.24] Denegación de servicio	[D]	[9]	[9]	50%	[8]	33	{7,1}
[019] [LAN] red local	[A.26] Ataque destructivo	[D]	[9]	[9]	100%	[9]	1,47	{6,4}
[019] [LAN] red local	[A.25] Robo de equipos	[D]	[9]	[9]	100%	[9]	1,18	{6,3}
[019] [LAN] red local	[I.6] Corte del suministro eléctrico	[D]	[9]	[9]	100%	[9]	1,05	{6,3}
[019] [LAN] red local	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	[9]	100%	[9]	1,05	{6,3}
[019] [LAN] red local	[A.18] Destrucción de la información	[D]	[9]	[9]	50%	[8]	3,6	{6,2}
[019] [LAN] red local	[A.7] Uso no previsto	[D]	[9]	[9]	50%	[8]	3,3	{6,2}

[019] [LAN] red local	[I.*] Desastres industriales	[D]	[9]	[9]	100%	[9]	0,52	{6,0}
[019] [LAN] red local	[I.1] Fuego	[D]	[9]	[9]	100%	[9]	0,52	{6,0}
[019] [LAN] red local	[E.24] Caída del sistema por agotamiento de recursos	[D]	[9]	[9]	50%	[8]	1,98	{6,0}
[019] [LAN] red local	[A.23] Manipulación del hardware	[D]	[9]	[9]	50%	[8]	1,47	{5,9}
[019] [LAN] red local	[I.8] Fallo de servicios de comunicaciones	[D]	[9]	[9]	50%	[8]	1,05	{5,7}
[019] [LAN] red local	[I.5] Avería de origen físico o lógico	[D]	[9]	[9]	50%	[8]	1,05	{5,7}
[019] [LAN] red local	[I.2] Daños por agua	[D]	[9]	[9]	50%	[8]	0,52	{5,5}
[019] [LAN] red local	[N.*] Desastres naturales	[D]	[9]	[9]	100%	[9]	0,105	{5,4}
[019] [LAN] red local	[N.1] Fuego	[D]	[9]	[9]	100%	[9]	0,105	{5,4}
[019] [LAN] red local	[E.25] Pérdida de equipos	[D]	[9]	[9]	20%	[7]	1,98	{5,3}
[019] [LAN] red local	[E.2] Errores del administrador del sistema / de la seguridad	[D]	[9]	[9]	20%	[7]	1,05	{5,0}
[019] [LAN] red local	[E.2] Errores del administrador del sistema / de la seguridad	[I]	[9]	[9]	20%	[7]	1,05	{5,0}
[019] [LAN] red local	[A.5] Suplantación de la identidad	[I]	[9]	[9]	10%	[6]	3,6	{5,0}
[019] [LAN] red local	[A.11] Acceso no autorizado	[D]	[9]	[9]	10%	[6]	3,6	{5,0}
[019] [LAN] red local	[A.11] Acceso no autorizado	[I]	[9]	[9]	10%	[6]	3,6	{5,0}
[019] [LAN] red local	[A.15] Modificación de la información	[I]	[9]	[9]	10%	[6]	3,6	{5,0}
[019] [LAN] red local	[I.3] Contaminación medioambiental	[D]	[9]	[9]	50%	[8]	0,105	{4,9}

[019] [LAN] red local	[N.2] Daños por agua	[D]	[9]	[9]	50%	[8]	0,105	{4,9}
[019] [LAN] red local	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D]	[9]	[9]	10%	[6]	1,98	{4,7}
[019] [LAN] red local	[A.10] Alteración de secuencia	[I]	[9]	[9]	10%	[6]	1,91	{4,7}
[019] [LAN] red local	[E.10] Errores de secuencia	[I]	[9]	[9]	10%	[6]	1,05	{4,5}
[019] [LAN] red local	[I.4] Contaminación electromagnética	[D]	[9]	[9]	10%	[6]	0,52	{4,2}
[019] [LAN] red local	[A.7] Uso no previsto	[I]	[9]	[9]	1%	[3]	3,3	{3,2}
[019] [LAN] red local	[E.15] Alteración de la información	[I]	[9]	[9]	1%	[3]	1,98	{3,0}
[020] [WIFI] red inalámbrica	[A.24] Denegación de servicio	[D]	[2]	[2]	50%	[1]	33	{2,9}
[020] [WIFI] red inalámbrica	[A.26] Ataque destructivo	[D]	[2]	[2]	100%	[2]	1,47	{2,3}
[020] [WIFI] red inalámbrica	[A.25] Robo de equipos	[D]	[2]	[2]	100%	[2]	1,18	{2,2}
[020] [WIFI] red inalámbrica	[I.6] Corte del suministro eléctrico	[D]	[2]	[2]	100%	[2]	1,05	{2,1}
[020] [WIFI] red inalámbrica	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[2]	[2]	100%	[2]	1,05	{2,1}
[020] [WIFI] red inalámbrica	[A.18] Destrucción de la información	[D]	[2]	[2]	50%	[1]	3,6	{2,1}
[020] [WIFI] red inalámbrica	[A.7] Uso no previsto	[D]	[2]	[2]	50%	[1]	3,3	{2,1}
[020] [WIFI] red inalámbrica	[I.1] Fuego	[D]	[2]	[2]	100%	[2]	0,52	{1,9}

[020] [WIFI] red inalámbrica	[I.*] Desastres industriales	[D]	[2]	[2]	100%	[2]	0,52	{1,9}
[020] [WIFI] red inalámbrica	[E.24] Caída del sistema por agotamiento de recursos	[D]	[2]	[2]	50%	[1]	1,98	{1,9}
[020] [WIFI] red inalámbrica	[A.23] Manipulación del hardware	[D]	[2]	[2]	50%	[1]	1,47	{1,7}
[020] [WIFI] red inalámbrica	[I.8] Fallo de servicios de comunicaciones	[D]	[2]	[2]	50%	[1]	1,05	{1,6}
[020] [WIFI] red inalámbrica	[I.5] Avería de origen físico o lógico	[D]	[2]	[2]	50%	[1]	1,05	{1,6}
[020] [WIFI] red inalámbrica	[N.1] Fuego	[D]	[2]	[2]	100%	[2]	0,105	{1,3}
[020] [WIFI] red inalámbrica	[N.*] Desastres naturales	[D]	[2]	[2]	100%	[2]	0,105	{1,3}
[020] [WIFI] red inalámbrica	[I.2] Daños por agua	[D]	[2]	[2]	50%	[1]	0,52	{1,3}
[020] [WIFI] red inalámbrica	[E.25] Pérdida de equipos	[D]	[2]	[2]	20%	[0]	1,98	{1,2}
[020] [WIFI] red inalámbrica	[E.2] Errores del administrador del sistema / de la seguridad	[D]	[2]	[2]	20%	[0]	1,05	{0,98}
[020] [WIFI] red inalámbrica	[A.11] Acceso no autorizado	[D]	[2]	[2]	10%	[0]	3,6	{0,97}
[020] [WIFI] red inalámbrica	[N.2] Daños por agua	[D]	[2]	[2]	50%	[1]	0,105	{0,94}
[020] [WIFI] red inalámbrica	[I.3] Contaminación medioambiental	[D]	[2]	[2]	50%	[1]	0,105	{0,94}
[020] [WIFI] red inalámbrica	[E.23] Errores de mantenimiento / actualización de equipos	[D]	[2]	[2]	10%	[0]	1,98	{0,92}

	(hardware)							
[020] [WIFI] red inalámbrica	[I.4] Contaminación electromagnética	[D]	[2]	[2]	10%	[0]	0,52	{0,82}
[021] [UPS_SERVIDOR] sistemas de alimentación ininterrumpida de 2 KVA en el servidor	[A.26] Ataque destructivo	[D]	[7]	[7]	100%	[7]	1,47	{5,2}
[021] [UPS_SERVIDOR] sistemas de alimentación ininterrumpida de 2 KVA en el servidor	[A.25] Robo de equipos	[D]	[7]	[7]	100%	[7]	1,18	{5,1}
[021] [UPS_SERVIDOR] sistemas de alimentación ininterrumpida de 2 KVA en el servidor	[A.23] Manipulación del hardware	[D]	[7]	[7]	50%	[6]	1,47	{4,7}
[021] [UPS_SERVIDOR] sistemas de alimentación ininterrumpida de 2 KVA en el servidor	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D]	[7]	[7]	10%	[4]	1,98	{3,6}
[021] [UPS_SERVIDOR] sistemas de alimentación ininterrumpida de 2 KVA en el servidor	[I.4] Contaminación electromagnética	[D]	[7]	[7]	10%	[4]	0,52	{3,1}
[021] [UPS_SERVIDOR] sistemas de alimentación ininterrumpida de 2 KVA en el servidor	[A.7] Uso no previsto	[D]	[7]	[7]	1%	[1]	3,3	{2,0}
[021] [UPS_SERVIDOR] sistemas de alimentación ininterrumpida de 2 KVA en el servidor	[I.2] Daños por agua	[D]	[7]	[7]	1%	[1]	0,52	{1,3}

[021] [UPS_SERVIDOR] sistemas de alimentación ininterrumpida de 2 KVA en el servidor	[I.*] Desastres industriales	[D]	[7]	[7]	1%	[1]	0,52	{1,3}
[021] [UPS_SERVIDOR] sistemas de alimentación ininterrumpida de 2 KVA en el servidor	[I.1] Fuego	[D]	[7]	[7]	1%	[1]	0,52	{1,3}
[021] [UPS_SERVIDOR] sistemas de alimentación ininterrumpida de 2 KVA en el servidor	[N.*] Desastres naturales	[D]	[7]	[7]	1%	[1]	0,105	{0,93}
[021] [UPS_SERVIDOR] sistemas de alimentación ininterrumpida de 2 KVA en el servidor	[I.3] Contaminación medioambiental	[D]	[7]	[7]	1%	[1]	0,105	{0,93}
[021] [UPS_SERVIDOR] sistemas de alimentación ininterrumpida de 2 KVA en el servidor	[N.2] Daños por agua	[D]	[7]	[7]	1%	[1]	0,105	{0,93}
[021] [UPS_SERVIDOR] sistemas de alimentación ininterrumpida de 2 KVA en el servidor	[N.1] Fuego	[D]	[7]	[7]	1%	[1]	0,105	{0,93}
[023] [ADSL] Conexión a internet brindada por un ISP	[A.24] Denegación de servicio	[D]	[9]	[9]	50%	[8]	33	{7,1}
[023] [ADSL] Conexión a internet brindada por un ISP	[A.18] Destrucción de la información	[D]	[9]	[9]	50%	[8]	3,6	{6,2}
[023] [ADSL] Conexión a internet brindada por un	[E.24] Caída del sistema por agotamiento de	[D]	[9]	[9]	50%	[8]	1,98	{6,0}

ISP	recursos							
[023] [ADSL] Conexión a internet brindada por un ISP	[I.8] Fallo de servicios de comunicaciones	[D]	[9]	[9]	50%	[8]	1,05	{5,7}
[023] [ADSL] Conexión a internet brindada por un ISP	[E.2] Errores del administrador del sistema / de la seguridad	[D]	[9]	[9]	20%	[7]	1,05	{5,0}
[023] [ADSL] Conexión a internet brindada por un ISP	[A.7] Uso no previsto	[D]	[9]	[9]	10%	[6]	3,3	{4,9}
[023] [ADSL] Conexión a internet brindada por un ISP	[E.18] Destrucción de la información	[D]	[9]	[9]	10%	[6]	1,98	{4,7}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[A.24] Denegación de servicio	[D]	[8]	[8]	100%	[8]	6,6	{6,4}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[E.24] Caída del sistema por agotamiento de recursos	[D]	[8]	[8]	50%	[7]	19,8	{6,3}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[A.8] Difusión de software dañino	[D]	[8]	[8]	100%	[8]	3,6	{6,2}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[A.8] Difusión de software dañino	[I]	[8]	[8]	100%	[8]	3,6	{6,2}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y	[A.22] Manipulación de programas	[I]	[8]	[8]	100%	[8]	3,3	{6,1}

financiera								
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[E.25] Pérdida de equipos	[D]	[8]	[8]	100%	[8]	1,98	{5,9}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[A.26] Ataque destructivo	[D]	[8]	[8]	100%	[8]	1,47	{5,8}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[I.6] Corte del suministro eléctrico	[D]	[8]	[8]	100%	[8]	1,05	{5,7}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[8]	[8]	100%	[8]	1,05	{5,7}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[A.22] Manipulación de programas	[D]	[8]	[8]	50%	[7]	3,3	{5,6}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[A.25] Robo de equipos	[D]	[8]	[8]	100%	[8]	0,74	{5,5}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[I.*] Desastres industriales	[D]	[8]	[8]	100%	[8]	0,52	{5,4}

[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[I.1] Fuego	[D]	[8]	[8]	100%	[8]	0,52	{5,4}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[I.5] Avería de origen físico o lógico	[D]	[8]	[8]	50%	[7]	1,05	{5,1}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[A.23] Manipulación del hardware	[D]	[8]	[8]	50%	[7]	0,74	{5,0}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[I.2] Daños por agua	[D]	[8]	[8]	50%	[7]	0,52	{4,9}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[N.1] Fuego	[D]	[8]	[8]	100%	[8]	0,105	{4,8}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[N.*] Desastres naturales	[D]	[8]	[8]	100%	[8]	0,105	{4,8}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[E.20] Vulnerabilidades de los programas (software)	[I]	[8]	[8]	20%	[6]	1,05	{4,4}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[A.11] Acceso no autorizado	[D]	[8]	[8]	10%	[5]	3,6	{4,4}

[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[A.11] Acceso no autorizado	[I]	[8]	[8]	10%	[5]	3,6	{4,4}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[A.8] Difusión de software dañino	[C]	[5]	[5]	100%	[5]	3,6	{4,4}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[N.2] Daños por agua	[D]	[8]	[8]	50%	[7]	0,105	{4,3}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[I.3] Contaminación medioambiental	[D]	[8]	[8]	50%	[7]	0,105	{4,3}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[A.22] Manipulación de programas	[C]	[5]	[5]	100%	[5]	3,3	{4,3}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D]	[8]	[8]	10%	[5]	1,98	{4,2}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[E.25] Pérdida de equipos	[C]	[5]	[5]	100%	[5]	1,98	{4,2}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[E.8] Difusión de software dañino	[D]	[8]	[8]	10%	[5]	1,98	{4,2}

[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[E.8] Difusión de software dañino	[I]	[8]	[8]	10%	[5]	1,98	{4,2}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[I.4] Contaminación electromagnética	[D]	[8]	[8]	10%	[5]	1,05	{3,9}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[A.11] Acceso no autorizado	[C]	[5]	[5]	50%	[4]	3,6	{3,9}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[A.25] Robo de equipos	[C]	[5]	[5]	100%	[5]	0,74	{3,8}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[E.21] Errores de mantenimiento / actualización de programas (software)	[D]	[8]	[8]	1%	[2]	19,8	{3,3}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[E.21] Errores de mantenimiento / actualización de programas (software)	[I]	[8]	[8]	1%	[2]	19,8	{3,3}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[A.23] Manipulación del hardware	[C]	[5]	[5]	50%	[4]	0,74	{3,2}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[E.20] Vulnerabilidades de los programas (software)	[C]	[5]	[5]	20%	[3]	1,05	{2,7}

[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[A.7] Uso no previsto	[D]	[8]	[8]	1%	[2]	3,3	{2,6}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[A.7] Uso no previsto	[C]	[5]	[5]	10%	[2]	3,3	{2,6}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[A.7] Uso no previsto	[I]	[8]	[8]	1%	[2]	3,3	{2,6}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[E.8] Difusión de software dañino	[C]	[5]	[5]	10%	[2]	1,98	{2,4}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[E.20] Vulnerabilidades de los programas (software)	[D]	[8]	[8]	1%	[2]	1,05	{2,1}
[003] [SW_GENERAL LEDGER] Sistema de Información contable y financiera	[I.11] Emanaciones electromagnéticas	[C]	[5]	[5]	1%	[0]	1,05	{0,87}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.24] Denegación de servicio	[D]	[10]	[10]	50%	[9]	33	{7,6}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios	[A.8] Difusión de software dañino	[D]	[10]	[10]	100%	[10]	3,6	{7,3}

de equipos y planes de Claro móvil								
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.8] Difusión de software dañino	[I]	[10]	[10]	100%	[10]	3,6	{7,3}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.22] Manipulación de programas	[I]	[10]	[10]	100%	[10]	3,3	{7,3}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.18] Destrucción de la información	[D]	[10]	[10]	50%	[9]	3,6	{6,8}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.22] Manipulación de programas	[D]	[10]	[10]	50%	[9]	3,3	{6,8}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[E.24] Caída del sistema por agotamiento de recursos	[D]	[10]	[10]	50%	[9]	1,98	{6,6}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de	[I.5] Avería de origen físico o lógico	[D]	[10]	[10]	50%	[9]	1,05	{6,3}

Claro móvil								
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[I.8] Fallo de servicios de comunicaciones	[D]	[10]	[10]	50%	[9]	1,05	{6,3}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.5] Suplantación de la identidad	[A]	[8]	[8]	100%	[8]	3,6	{6,2}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.11] Acceso no autorizado	[A]	[8]	[8]	100%	[8]	3,6	{6,2}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[E.2] Errores del administrador del sistema / de la seguridad	[D]	[10]	[10]	20%	[8]	1,05	{5,6}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[E.2] Errores del administrador del sistema / de la seguridad	[I]	[10]	[10]	20%	[8]	1,05	{5,6}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de	[E.20] Vulnerabilidades de los programas (software)	[I]	[10]	[10]	20%	[8]	1,05	{5,6}

Claro móvil								
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.5] Suplantación de la identidad	[I]	[10]	[10]	10%	[7]	3,6	{5,6}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.11] Acceso no autorizado	[I]	[10]	[10]	10%	[7]	3,6	{5,6}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.15] Modificación de la información	[I]	[10]	[10]	10%	[7]	3,6	{5,6}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.7] Uso no previsto	[D]	[10]	[10]	10%	[7]	3,3	{5,5}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.7] Uso no previsto	[I]	[10]	[10]	10%	[7]	3,3	{5,5}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de	[E.8] Difusión de software dañino	[D]	[10]	[10]	10%	[7]	1,98	{5,3}

Claro móvil								
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[E.8] Difusión de software dañino	[I]	[10]	[10]	10%	[7]	1,98	{5,3}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.10] Alteración de secuencia	[I]	[10]	[10]	10%	[7]	1,91	{5,3}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[E.10] Errores de secuencia	[I]	[10]	[10]	10%	[7]	1,05	{5,1}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.8] Difusión de software dañino	[C]	[5]	[5]	100%	[5]	3,6	{4,4}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[E.21] Errores de mantenimiento / actualización de programas (software)	[D]	[10]	[10]	1%	[4]	19,8	{4,4}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de	[E.21] Errores de mantenimiento / actualización de programas (software)	[I]	[10]	[10]	1%	[4]	19,8	{4,4}

Claro móvil								
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.22] Manipulación de programas	[C]	[5]	[5]	100%	[5]	3,3	{4,3}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.5] Suplantación de la identidad	[C]	[5]	[5]	50%	[4]	3,6	{3,9}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.11] Acceso no autorizado	[C]	[5]	[5]	50%	[4]	3,6	{3,9}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[E.15] Alteración de la información	[I]	[10]	[10]	1%	[4]	1,98	{3,6}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[E.20] Vulnerabilidades de los programas (software)	[D]	[10]	[10]	1%	[4]	1,05	{3,3}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de	[E.2] Errores del administrador del sistema / de la seguridad	[C]	[5]	[5]	20%	[3]	1,05	{2,7}

Claro móvil								
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[E.20] Vulnerabilidades de los programas (software)	[C]	[5]	[5]	20%	[3]	1,05	{2,7}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.7] Uso no previsto	[C]	[5]	[5]	10%	[2]	3,3	{2,6}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[E.19] Fugas de información	[C]	[5]	[5]	10%	[2]	1,98	{2,4}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[E.8] Difusión de software dañino	[C]	[5]	[5]	10%	[2]	1,98	{2,4}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.9] [Re-]encaminamiento de mensajes	[C]	[5]	[5]	10%	[2]	1,91	{2,4}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de	[E.9] Errores de [re-]encaminamiento	[C]	[5]	[5]	10%	[2]	1,05	{2,1}

Claro móvil								
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.14] Interceptación de información (escucha)	[C]	[5]	[5]	5%	[1]	3,6	{2,1}
[004] [PL_POLIEDRO] Plataforma Poliedro información de precios de equipos y planes de Claro móvil	[A.12] Análisis de tráfico	[C]	[5]	[5]	2%	[0]	1,91	{1,1}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[A.24] Denegación de servicio	[D]	[5]	[5]	100%	[5]	6,6	{4,6}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[E.24] Caída del sistema por agotamiento de recursos	[D]	[5]	[5]	50%	[4]	19,8	{4,5}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[A.8] Difusión de software dañino	[D]	[5]	[5]	100%	[5]	3,6	{4,4}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[A.8] Difusión de software dañino	[I]	[5]	[5]	100%	[5]	3,6	{4,4}
[005] [SW_CELSIS] Sistema de información y registro de clientes y	[A.22] Manipulación de programas	[I]	[5]	[5]	100%	[5]	3,3	{4,3}

ventas								
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[E.25] Pérdida de equipos	[D]	[5]	[5]	100%	[5]	1,98	{4,2}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[A.26] Ataque destructivo	[D]	[5]	[5]	100%	[5]	1,47	{4,0}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[I.6] Corte del suministro eléctrico	[D]	[5]	[5]	100%	[5]	1,05	{3,9}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[5]	[5]	100%	[5]	1,05	{3,9}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[A.25] Robo de equipos	[D]	[5]	[5]	100%	[5]	0,74	{3,8}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[A.22] Manipulación de programas	[D]	[5]	[5]	50%	[4]	3,3	{3,8}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[I.1] Fuego	[D]	[5]	[5]	100%	[5]	0,52	{3,6}

[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[I.*] Desastres industriales	[D]	[5]	[5]	100%	[5]	0,52	{3,6}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[I.5] Avería de origen físico o lógico	[D]	[5]	[5]	50%	[4]	1,05	{3,4}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[A.23] Manipulación del hardware	[D]	[5]	[5]	50%	[4]	0,74	{3,2}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[I.2] Daños por agua	[D]	[5]	[5]	50%	[4]	0,52	{3,1}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[N.1] Fuego	[D]	[5]	[5]	100%	[5]	0,105	{3,0}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[N.*] Desastres naturales	[D]	[5]	[5]	100%	[5]	0,105	{3,0}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[E.20] Vulnerabilidades de los programas (software)	[I]	[5]	[5]	20%	[3]	1,05	{2,7}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[A.11] Acceso no autorizado	[D]	[5]	[5]	10%	[2]	3,6	{2,6}

[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[A.11] Acceso no autorizado	[I]	[5]	[5]	10%	[2]	3,6	{2,6}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[A.8] Difusión de software dañino	[C]	[2]	[2]	100%	[2]	3,6	{2,6}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[A.22] Manipulación de programas	[C]	[2]	[2]	100%	[2]	3,3	{2,6}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[N.2] Daños por agua	[D]	[5]	[5]	50%	[4]	0,105	{2,5}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[I.3] Contaminación medioambiental	[D]	[5]	[5]	50%	[4]	0,105	{2,5}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D]	[5]	[5]	10%	[2]	1,98	{2,4}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[E.25] Pérdida de equipos	[C]	[2]	[2]	100%	[2]	1,98	{2,4}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[E.8] Difusión de software dañino	[D]	[5]	[5]	10%	[2]	1,98	{2,4}

[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[E.8] Difusión de software dañino	[I]	[5]	[5]	10%	[2]	1,98	{2,4}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[I.4] Contaminación electromagnética	[D]	[5]	[5]	10%	[2]	1,05	{2,1}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[A.11] Acceso no autorizado	[C]	[2]	[2]	50%	[1]	3,6	{2,1}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[A.25] Robo de equipos	[C]	[2]	[2]	100%	[2]	0,74	{2,0}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[A.23] Manipulación del hardware	[C]	[2]	[2]	50%	[1]	0,74	{1,5}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[E.21] Errores de mantenimiento / actualización de programas (software)	[D]	[5]	[5]	1%	[0]	19,8	{1,5}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[E.21] Errores de mantenimiento / actualización de programas (software)	[I]	[5]	[5]	1%	[0]	19,8	{1,5}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[E.20] Vulnerabilidades de los programas (software)	[C]	[2]	[2]	20%	[0]	1,05	{0,98}

[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[A.7] Uso no previsto	[D]	[5]	[5]	1%	[0]	3,3	{0,96}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[A.7] Uso no previsto	[C]	[2]	[2]	10%	[0]	3,3	{0,96}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[A.7] Uso no previsto	[I]	[5]	[5]	1%	[0]	3,3	{0,96}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[E.8] Difusión de software dañino	[C]	[2]	[2]	10%	[0]	1,98	{0,92}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[E.20] Vulnerabilidades de los programas (software)	[D]	[5]	[5]	1%	[0]	1,05	{0,87}
[005] [SW_CELSIS] Sistema de información y registro de clientes y ventas	[I.11] Emanaciones electromagnéticas	[C]	[2]	[2]	1%	[0]	1,05	{0,52}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[A.24] Denegación de servicio	[D]	[10]	[10]	100%	[10]	6,6	{7,6}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[E.24] Caída del sistema por agotamiento de recursos	[D]	[10]	[10]	50%	[9]	19,8	{7,4}

[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[A.8] Difusión de software dañino	[D]	[10]	[10]	100%	[10]	3,6	{7,3}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[A.8] Difusión de software dañino	[I]	[10]	[10]	100%	[10]	3,6	{7,3}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[A.22] Manipulación de programas	[I]	[10]	[10]	100%	[10]	3,3	{7,3}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[E.25] Pérdida de equipos	[D]	[10]	[10]	100%	[10]	1,98	{7,1}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[A.26] Ataque destructivo	[D]	[10]	[10]	100%	[10]	1,47	{7,0}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[I.6] Corte del suministro eléctrico	[D]	[10]	[10]	100%	[10]	1,05	{6,9}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[10]	[10]	100%	[10]	1,05	{6,9}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[A.22] Manipulación de programas	[D]	[10]	[10]	50%	[9]	3,3	{6,8}

[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[A.25] Robo de equipos	[D]	[10]	[10]	100%	[10]	0,74	{6,7}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[I.*] Desastres industriales	[D]	[10]	[10]	100%	[10]	0,52	{6,6}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[I.1] Fuego	[D]	[10]	[10]	100%	[10]	0,52	{6,6}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[I.5] Avería de origen físico o lógico	[D]	[10]	[10]	50%	[9]	1,05	{6,3}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[A.23] Manipulación del hardware	[D]	[10]	[10]	50%	[9]	0,74	{6,2}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[I.2] Daños por agua	[D]	[10]	[10]	50%	[9]	0,52	{6,1}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[N.1] Fuego	[D]	[10]	[10]	100%	[10]	0,105	{6,0}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[N.*] Desastres naturales	[D]	[10]	[10]	100%	[10]	0,105	{6,0}

[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[E.20] Vulnerabilidades de los programas (software)	[I]	[10]	[10]	20%	[8]	1,05	{5,6}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[A.11] Acceso no autorizado	[D]	[10]	[10]	10%	[7]	3,6	{5,6}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[A.11] Acceso no autorizado	[I]	[10]	[10]	10%	[7]	3,6	{5,6}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[N.2] Daños por agua	[D]	[10]	[10]	50%	[9]	0,105	{5,4}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[I.3] Contaminación medioambiental	[D]	[10]	[10]	50%	[9]	0,105	{5,4}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D]	[10]	[10]	10%	[7]	1,98	{5,3}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[E.8] Difusión de software dañino	[D]	[10]	[10]	10%	[7]	1,98	{5,3}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[E.8] Difusión de software dañino	[I]	[10]	[10]	10%	[7]	1,98	{5,3}

[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[I.4] Contaminación electromagnética	[D]	[10]	[10]	10%	[7]	1,05	{5,1}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[A.8] Difusión de software dañino	[C]	[5]	[5]	100%	[5]	3,6	{4,4}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[E.21] Errores de mantenimiento / actualización de programas (software)	[D]	[10]	[10]	1%	[4]	19,8	{4,4}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[E.21] Errores de mantenimiento / actualización de programas (software)	[I]	[10]	[10]	1%	[4]	19,8	{4,4}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[A.22] Manipulación de programas	[C]	[5]	[5]	100%	[5]	3,3	{4,3}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[E.25] Pérdida de equipos	[C]	[5]	[5]	100%	[5]	1,98	{4,2}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[A.11] Acceso no autorizado	[C]	[5]	[5]	50%	[4]	3,6	{3,9}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[A.25] Robo de equipos	[C]	[5]	[5]	100%	[5]	0,74	{3,8}

[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[A.7] Uso no previsto	[D]	[10]	[10]	1%	[4]	3,3	{3,8}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[A.7] Uso no previsto	[I]	[10]	[10]	1%	[4]	3,3	{3,8}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[E.20] Vulnerabilidades de los programas (software)	[D]	[10]	[10]	1%	[4]	1,05	{3,3}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[A.23] Manipulación del hardware	[C]	[5]	[5]	50%	[4]	0,74	{3,2}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[E.20] Vulnerabilidades de los programas (software)	[C]	[5]	[5]	20%	[3]	1,05	{2,7}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[A.7] Uso no previsto	[C]	[5]	[5]	10%	[2]	3,3	{2,6}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[E.8] Difusión de software dañino	[C]	[5]	[5]	10%	[2]	1,98	{2,4}
[006] [SQL_SERVER] sistema de gestión de bases de datos relacionales	[I.11] Emanaciones electromagnéticas	[C]	[5]	[5]	1%	[0]	1,05	{0,87}

[007] [SO] Sistema Operativo	[A.8] Difusión de software dañino	[D]	[7]	[7]	100%	[7]	3,6	{5,6}
[007] [SO] Sistema Operativo	[A.8] Difusión de software dañino	[I]	[7]	[7]	100%	[7]	3,6	{5,6}
[007] [SO] Sistema Operativo	[A.22] Manipulación de programas	[I]	[7]	[7]	100%	[7]	3,3	{5,5}
[007] [SO] Sistema Operativo	[A.22] Manipulación de programas	[D]	[7]	[7]	50%	[6]	3,3	{5,0}
[007] [SO] Sistema Operativo	[I.5] Avería de origen físico o lógico	[D]	[7]	[7]	50%	[6]	1,05	{4,6}
[007] [SO] Sistema Operativo	[A.8] Difusión de software dañino	[C]	[5]	[5]	100%	[5]	3,6	{4,4}
[007] [SO] Sistema Operativo	[A.22] Manipulación de programas	[C]	[5]	[5]	100%	[5]	3,3	{4,3}
[007] [SO] Sistema Operativo	[E.20] Vulnerabilidades de los programas (software)	[I]	[7]	[7]	20%	[5]	1,05	{3,9}
[007] [SO] Sistema Operativo	[E.8] Difusión de software dañino	[D]	[7]	[7]	10%	[4]	1,98	{3,6}
[007] [SO] Sistema Operativo	[E.8] Difusión de software dañino	[I]	[7]	[7]	10%	[4]	1,98	{3,6}
[007] [SO] Sistema Operativo	[E.20] Vulnerabilidades de los programas (software)	[C]	[5]	[5]	20%	[3]	1,05	{2,7}
[007] [SO] Sistema Operativo	[E.21] Errores de mantenimiento / actualización de programas (software)	[D]	[7]	[7]	1%	[1]	19,8	{2,7}
[007] [SO] Sistema Operativo	[E.21] Errores de mantenimiento / actualización de programas (software)	[I]	[7]	[7]	1%	[1]	19,8	{2,7}
[007] [SO] Sistema	[E.8] Difusión de software	[C]	[5]	[5]	10%	[2]	1,98	{2,4}

Operativo	dañino							
[007] [SO] Sistema Operativo	[E.20] Vulnerabilidades de los programas (software)	[D]	[7]	[7]	1%	[1]	1,05	{1,6}
[008] [OFFICE] ofimática	[A.8] Difusión de software dañino	[D]	[1]	[1]	100%	[1]	3,6	{2,0}
[008] [OFFICE] ofimática	[A.8] Difusión de software dañino	[I]	[1]	[1]	100%	[1]	3,6	{2,0}
[008] [OFFICE] ofimática	[A.22] Manipulación de programas	[I]	[1]	[1]	100%	[1]	3,3	{2,0}
[008] [OFFICE] ofimática	[A.22] Manipulación de programas	[D]	[1]	[1]	50%	[0]	3,3	{1,5}
[008] [OFFICE] ofimática	[I.5] Avería de origen físico o lógico	[D]	[1]	[1]	50%	[0]	1,05	{1,0}
[008] [OFFICE] ofimática	[E.20] Vulnerabilidades de los programas (software)	[I]	[1]	[1]	20%	[0]	1,05	{0,86}
[008] [OFFICE] ofimática	[E.8] Difusión de software dañino	[D]	[1]	[1]	10%	[0]	1,98	{0,80}
[008] [OFFICE] ofimática	[E.8] Difusión de software dañino	[I]	[1]	[1]	10%	[0]	1,98	{0,80}
[008] [OFFICE] ofimática	[E.21] Errores de mantenimiento / actualización de programas (software)	[D]	[1]	[1]	1%	[0]	19,8	{0,63}
[008] [OFFICE] ofimática	[E.21] Errores de mantenimiento / actualización de programas (software)	[I]	[1]	[1]	1%	[0]	19,8	{0,63}
[008] [OFFICE] ofimática	[E.20] Vulnerabilidades de los programas (software)	[D]	[1]	[1]	1%	[0]	1,05	{0,40}
[009] [AV] Anti virus	[A.8] Difusión de software dañino	[D]	[7]	[7]	100%	[7]	3,6	{5,6}

[009] [AV] Anti virus	[A.22] Manipulación de programas	[D]	[7]	[7]	50%	[6]	3,3	{5,0}
[009] [AV] Anti virus	[I.5] Avería de origen físico o lógico	[D]	[7]	[7]	50%	[6]	1,05	{4,6}
[009] [AV] Anti virus	[A.8] Difusión de software dañino	[I]	[4]	[4]	100%	[4]	3,6	{3,8}
[009] [AV] Anti virus	[A.8] Difusión de software dañino	[C]	[4]	[4]	100%	[4]	3,6	{3,8}
[009] [AV] Anti virus	[A.22] Manipulación de programas	[I]	[4]	[4]	100%	[4]	3,3	{3,8}
[009] [AV] Anti virus	[A.22] Manipulación de programas	[C]	[4]	[4]	100%	[4]	3,3	{3,8}
[009] [AV] Anti virus	[E.8] Difusión de software dañino	[D]	[7]	[7]	10%	[4]	1,98	{3,6}
[009] [AV] Anti virus	[E.21] Errores de mantenimiento / actualización de programas (software)	[D]	[7]	[7]	1%	[1]	19,8	{2,7}
[009] [AV] Anti virus	[E.20] Vulnerabilidades de los programas (software)	[I]	[4]	[4]	20%	[2]	1,05	{2,1}
[009] [AV] Anti virus	[E.20] Vulnerabilidades de los programas (software)	[C]	[4]	[4]	20%	[2]	1,05	{2,1}
[009] [AV] Anti virus	[E.8] Difusión de software dañino	[I]	[4]	[4]	10%	[1]	1,98	{1,8}
[009] [AV] Anti virus	[E.8] Difusión de software dañino	[C]	[4]	[4]	10%	[1]	1,98	{1,8}
[009] [AV] Anti virus	[E.20] Vulnerabilidades de los programas (software)	[D]	[7]	[7]	1%	[1]	1,05	{1,6}
[009] [AV] Anti virus	[E.21] Errores de mantenimiento / actualización de	[I]	[4]	[4]	1%	[0]	19,8	{0,98}

	programas (software)							
[022] [oficina] CELUTEL SAS SINCELEJO CENTRO	[A.27] Ocupación enemiga	[D]	[9]	[9]	100%	[9]	1,47	{6,4}
[022] [oficina] CELUTEL SAS SINCELEJO CENTRO	[N.1] Fuego	[D]	[9]	[9]	100%	[9]	1,05	{6,3}
[022] [oficina] CELUTEL SAS SINCELEJO CENTRO	[I.1] Fuego	[D]	[9]	[9]	100%	[9]	1,05	{6,3}
[022] [oficina] CELUTEL SAS SINCELEJO CENTRO	[I.*] Desastres industriales	[D]	[9]	[9]	100%	[9]	1,05	{6,3}
[022] [oficina] CELUTEL SAS SINCELEJO CENTRO	[I.2] Daños por agua	[D]	[9]	[9]	100%	[9]	1,05	{6,3}
[022] [oficina] CELUTEL SAS SINCELEJO CENTRO	[N.2] Daños por agua	[D]	[9]	[9]	100%	[9]	1,05	{6,3}
[022] [oficina] CELUTEL SAS SINCELEJO CENTRO	[N.*] Desastres naturales	[D]	[9]	[9]	100%	[9]	0,52	{6,0}
[022] [oficina] CELUTEL SAS SINCELEJO CENTRO	[A.26] Ataque destructivo	[D]	[9]	[9]	100%	[9]	0,147	{5,5}
[022] [oficina] CELUTEL SAS SINCELEJO CENTRO	[A.6] Abuso de privilegios de acceso	[D]	[9]	[9]	10%	[6]	3,3	{4,9}
[022] [oficina] CELUTEL SAS SINCELEJO CENTRO	[A.7] Uso no previsto	[D]	[9]	[9]	10%	[6]	3,3	{4,9}
[022] [oficina] CELUTEL SAS SINCELEJO CENTRO	[I.3] Contaminación medioambiental	[D]	[9]	[9]	10%	[6]	1,05	{4,5}
[022] [oficina] CELUTEL SAS SINCELEJO CENTRO	[I.4] Contaminación electromagnética	[D]	[9]	[9]	10%	[6]	0,105	{3,6}
[024] [IS] ingeniero de sistemas	[A.19] Revelación de información	[C]	[9]	[9]	50%	[8]	36	{7,1}
[024] [IS] ingeniero de sistemas	[A.29] Extorsión	[I]	[9]	[9]	100%	[9]	2,3	{6,6}
[024] [IS] ingeniero de sistemas	[A.29] Extorsión	[C]	[9]	[9]	100%	[9]	2,3	{6,6}

[024] [IS] ingeniero de sistemas	[A.30] Ingeniería social (picaresca)	[I]	[9]	[9]	100%	[9]	1,26	{6,3}
[024] [IS] ingeniero de sistemas	[A.30] Ingeniería social (picaresca)	[C]	[9]	[9]	100%	[9]	1,26	{6,3}
[024] [IS] ingeniero de sistemas	[A.15] Modificación de la información	[I]	[9]	[9]	50%	[8]	3,6	{6,2}
[024] [IS] ingeniero de sistemas	[A.29] Extorsión	[D]	[9]	[9]	50%	[8]	2,3	{6,0}
[024] [IS] ingeniero de sistemas	[A.30] Ingeniería social (picaresca)	[D]	[9]	[9]	50%	[8]	1,26	{5,8}
[024] [IS] ingeniero de sistemas	[A.18] Destrucción de la información	[D]	[9]	[9]	10%	[6]	3,6	{5,0}
[024] [IS] ingeniero de sistemas	[A.28] Indisponibilidad del personal	[D]	[9]	[9]	20%	[7]	0,67	{4,9}
[024] [IS] ingeniero de sistemas	[E.15] Alteración de la información	[I]	[9]	[9]	10%	[6]	1,98	{4,7}
[024] [IS] ingeniero de sistemas	[E.19] Fugas de información	[C]	[9]	[9]	10%	[6]	1,98	{4,7}
[024] [IS] ingeniero de sistemas	[E.28] Indisponibilidad del personal	[D]	[9]	[9]	10%	[6]	1,05	{4,5}
[024] [IS] ingeniero de sistemas	[E.18] Destrucción de la información	[D]	[9]	[9]	1%	[3]	1,98	{3,0}
[025] [USER_OP_CONT] contador	[A.15] Modificación de la información	[I]	[7]	[7]	50%	[6]	3,6	{5,0}
[025] [USER_OP_CONT] contador	[A.29] Extorsión	[I]	[7]	[7]	20%	[5]	2,3	{4,1}
[025] [USER_OP_CONT] contador	[A.30] Ingeniería social (picaresca)	[I]	[7]	[7]	20%	[5]	1,26	{3,9}
[025] [USER_OP_CONT] contador	[E.15] Alteración de la información	[I]	[7]	[7]	10%	[4]	1,98	{3,6}
[025] [USER_OP_CONT]	[A.28] Indisponibilidad del	[D]	[5]	[5]	50%	[4]	0,67	{3,2}

contador	personal							
[025] [USER_OP_CONT] contador	[A.18] Destrucción de la información	[D]	[5]	[5]	10%	[2]	3,6	{2,6}
[025] [USER_OP_CONT] contador	[A.29] Extorsión	[D]	[5]	[5]	10%	[2]	2,3	{2,4}
[025] [USER_OP_CONT] contador	[A.30] Ingeniería social (picaresca)	[D]	[5]	[5]	10%	[2]	1,26	{2,2}
[025] [USER_OP_CONT] contador	[E.28] Indisponibilidad del personal	[D]	[5]	[5]	10%	[2]	1,05	{2,1}
[025] [USER_OP_CONT] contador	[E.18] Destrucción de la información	[D]	[5]	[5]	1%	[0]	1,98	{0,92}
[026] [USER_OP_BOD] administrador bodega	[A.15] Modificación de la información	[I]	[7]	[7]	50%	[6]	3,6	{5,0}
[026] [USER_OP_BOD] administrador bodega	[A.29] Extorsión	[I]	[7]	[7]	20%	[5]	2,3	{4,1}
[026] [USER_OP_BOD] administrador bodega	[A.30] Ingeniería social (picaresca)	[I]	[7]	[7]	20%	[5]	1,26	{3,9}
[026] [USER_OP_BOD] administrador bodega	[E.15] Alteración de la información	[I]	[7]	[7]	10%	[4]	1,98	{3,6}
[026] [USER_OP_BOD] administrador bodega	[A.28] Indisponibilidad del personal	[D]	[5]	[5]	50%	[4]	0,67	{3,2}
[026] [USER_OP_BOD] administrador bodega	[A.18] Destrucción de la información	[D]	[5]	[5]	10%	[2]	3,6	{2,6}
[026] [USER_OP_BOD] administrador bodega	[A.29] Extorsión	[D]	[5]	[5]	10%	[2]	2,3	{2,4}
[026] [USER_OP_BOD] administrador bodega	[A.30] Ingeniería social (picaresca)	[D]	[5]	[5]	10%	[2]	1,26	{2,2}
[026] [USER_OP_BOD] administrador bodega	[E.28] Indisponibilidad del personal	[D]	[5]	[5]	10%	[2]	1,05	{2,1}
[026] [USER_OP_BOD] administrador bodega	[E.18] Destrucción de la información	[D]	[5]	[5]	1%	[0]	1,98	{0,92}

[027] [USER_OP_CAJA] cajero	[A.15] Modificación de la información	[I]	[7]	[7]	50%	[6]	3,6	{5,0}
[027] [USER_OP_CAJA] cajero	[A.29] Extorsión	[I]	[7]	[7]	20%	[5]	2,3	{4,1}
[027] [USER_OP_CAJA] cajero	[A.30] Ingeniería social (picaresca)	[I]	[7]	[7]	20%	[5]	1,26	{3,9}
[027] [USER_OP_CAJA] cajero	[E.15] Alteración de la información	[I]	[7]	[7]	10%	[4]	1,98	{3,6}
[027] [USER_OP_CAJA] cajero	[A.28] Indisponibilidad del personal	[D]	[5]	[5]	50%	[4]	0,67	{3,2}
[027] [USER_OP_CAJA] cajero	[A.18] Destrucción de la información	[D]	[5]	[5]	10%	[2]	3,6	{2,6}
[027] [USER_OP_CAJA] cajero	[A.29] Extorsión	[D]	[5]	[5]	10%	[2]	2,3	{2,4}
[027] [USER_OP_CAJA] cajero	[A.30] Ingeniería social (picaresca)	[D]	[5]	[5]	10%	[2]	1,26	{2,2}
[027] [USER_OP_CAJA] cajero	[E.28] Indisponibilidad del personal	[D]	[5]	[5]	10%	[2]	1,05	{2,1}
[027] [USER_OP_CAJA] cajero	[E.18] Destrucción de la información	[D]	[5]	[5]	1%	[0]	1,98	{0,92}
[028] [USER_OP_VENT] asesores comerciales	[A.28] Indisponibilidad del personal	[D]	[5]	[5]	50%	[4]	0,67	{3,2}
[028] [USER_OP_VENT] asesores comerciales	[A.18] Destrucción de la información	[D]	[5]	[5]	10%	[2]	3,6	{2,6}
[028] [USER_OP_VENT] asesores comerciales	[A.29] Extorsión	[D]	[5]	[5]	10%	[2]	2,3	{2,4}
[028] [USER_OP_VENT] asesores comerciales	[A.30] Ingeniería social (picaresca)	[D]	[5]	[5]	10%	[2]	1,26	{2,2}
[028] [USER_OP_VENT] asesores comerciales	[E.28] Indisponibilidad del personal	[D]	[5]	[5]	10%	[2]	1,05	{2,1}
[028] [USER_OP_VENT]	[E.18] Destrucción de la	[D]	[5]	[5]	1%	[0]	1,98	{0,92}

asesores comerciales	información							