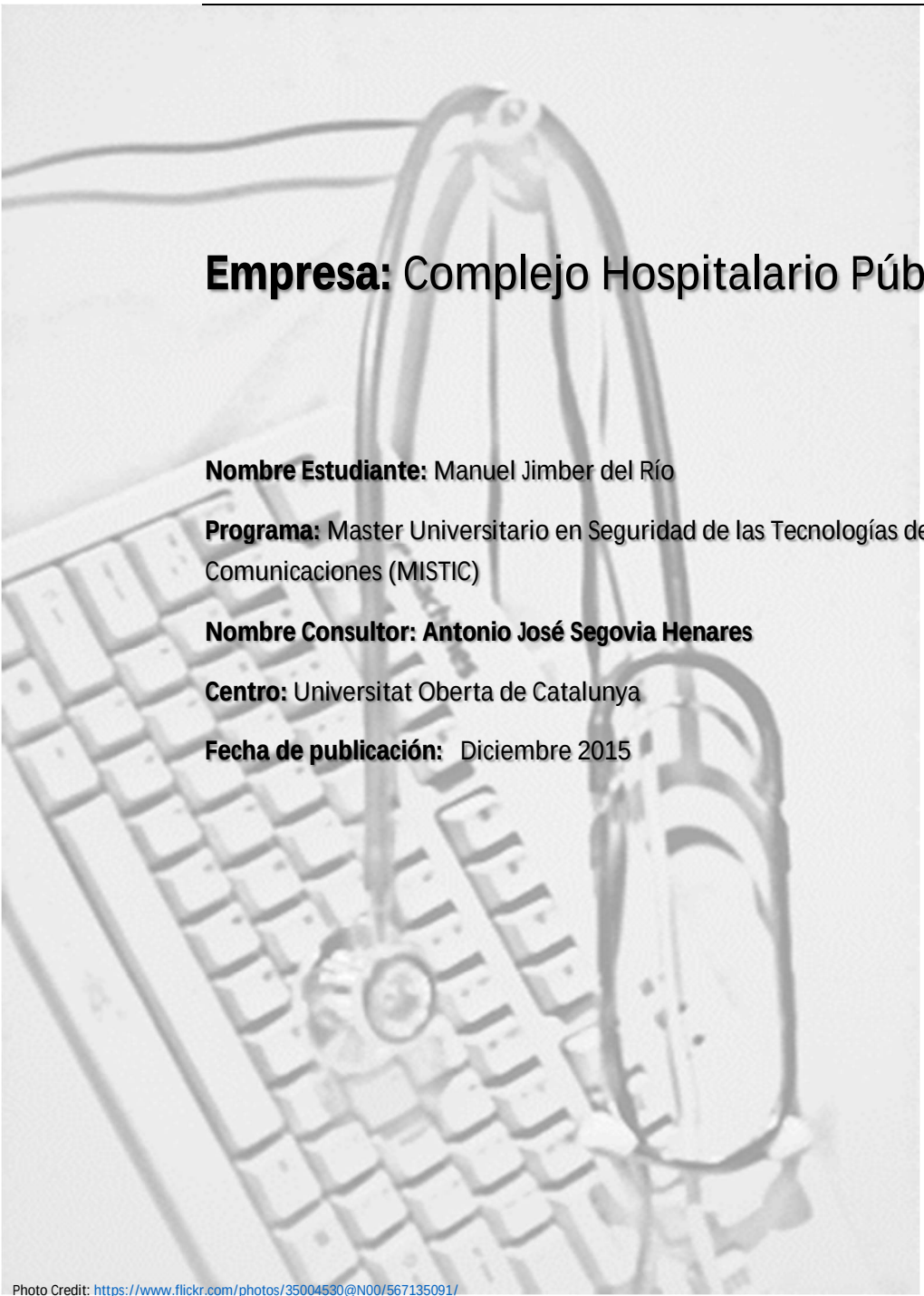
Plan Director de Seguridad de la Información Para el Servicio de Atención en Urgencias



Empresa: Complejo Hospitalario Público Provincial

Nombre Estudiante: Manuel Jimber del Río

Programa: Master Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Nombre Consultor: Antonio José Segovia Henares

Centro: Universitat Oberta de Catalunya

Fecha de publicación: Diciembre 2015

Título del trabajo:	*Plan Director de Seguridad Para Servicio de Atención en Urgencias.*
Nombre del autor:	*Manuel Jimber del Río*
Nombre del consultor:	*Antonio José Segovia Henares*
Fecha de publicación:	*Diciembre 2015*
Área de Trabajo Final:	*Especialidad de Gestión y auditoría de la seguridad de la iinformación*
Titulación:	Master Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Resumen:

Este trabajo consiste en el desarrollo de un plan director de seguridad de la información de un servicio de atención en urgencias médicas en un complejo hospitalario de gran tamaño. El plan director se realiza de acuerdo a la norma ISO/IEC 27001 para la puesta en marcha de un SGSI y a la norma ISO/IEC 27002 como guía para la elaboración de la declaración de aplicablidad del plan. El plan director se desarrolla en 6 fases.

La primera fase consiste en una aproximación a la situación actual de la seguridad de la información de los sistemas de urgencias a través del análisis diferencial contra las normas ISO/IEC 27001 e ISO/IEC 27002. La segunda fase define todo el sistema de gestión documental y desarrolla los documentos y procedimientos nesesarios para el SGSI, destacando la política de seguridad y todos los procedimientos relacionados.

En la fase 3 hacemos un análisis de riesgos. Se identifican los activos involucrados en el proyecto, se calcula su valor y se hace un análisis cualitativo de las amenazas que puedan afectarles. A partir del valor de los activos y las amenazas calculamos el impacto potencial y el riesgo potencial. Considerando las salvaguardas actualmente vigentes, se calcula el impacto residual y riesgo residual.

En la fase 4 se describen las mejoras propuestas (proyectos) que deberán ayudar a mitigar el riesgo actual a la organización y evolucionar el cumplimiento ISO hasta un nivel adecuado. Dichos proyectos derivan de los resultados obtenidos del Análisis de Riesgos de acuerdo con las amenazas identificadas.

Llegados a la fase 5, conocemos los activos de la empresa y hemos evaluado las amenazas. Es el momento de hacer un alto en el camino y evaluar hasta que punto la empresa cumple con las buenas prácticas en materia de seguridad. La ISO/IEC 27002:2013 nos servirá como marco de control del estado de la seguridad.

This work involves the development of a master plan security information for a emergencies medical services in a large hospital complex. The master plan is made according to ISO / IEC 27001 for the implementation of an ISMS and ISO / IEC 27002 as a guide for the preparation of the statement of applicability for this plan. The master plan is developed in 6 stages. The first phase involves an approach to the current situation of information security emergency systems through differential analysis against ISO / IEC 27001 and ISO / IEC 27002 standards

The second phase defines the entire document management system and develops necessary documents and procedures for the ISMS, highlighting the security policy and all related procedures.

In phase 3 we do a risk analysis. We identify the assets involved in the project, calculate their value and make a qualitative analysis of the threats that may affect them. From the value of assets and threats first we calculate the potential impact and potential risk. We consider the safeguards currently in place and calculate the residual impact and residual risk.

In phase 4 proposed improvements (projects) that will help to mitigate the current risk to the organization and the ISO compliance evolve to a level suitable are described. These projects derived from the results of Risk Analysis according to the identified threats.

At phase 5, we know the assets of the company and we have assessed the threats. It's time to stop along the way and assess to what extent the company complies with good safety practices. The ISO / IEC 27002: 2013 will serve as a framework for monitoring the status of security.

Contenido

Lista de Tablas

Lista de Ilustraciones

FASE 1: Situación Actual: Contextualización, Objetivos y Análisis Diferencial

1. Introducción

El Plan Director de Seguridad es uno de los elementos clave con que debe trabajar el Responsable de Seguridad de una organización. Este plan constituye la hoja de ruta que debe seguir la empresa para gestionar de una forma adecuada la seguridad, permitiendo no sólo conocer el estado de la misma, sino en qué líneas se debe actuar para mejorarla. Estamos hablando por tanto de un modelo de mejora continua PDCA (Plan-Do-Check-Act) basado en el conocido ciclo de Deming.

El marco legal ha reflejado la importancia de la seguridad de la información (a nivel del estado español, leyes como la 11/2007 artículo 42: "Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad", lo demuestran) con su desarrollo en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, y en Andalucía el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

Otras leyes tales como la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica protegen de manera especial los datos de salud de los pacientes.

La seguridad no es por tanto un aspecto opcional, sino que debe ser inherente a las actividades de la propia organización, y constituye un punto de partida ineludible para toda organización en la actualidad.

Sin embargo, en nuestro caso, la seguridad de la información no es solo una cuestión legal, sino que también forma parte de las obligaciones de esta organización para con la seguridad de sus pacientes para la prestación de una asistencia sanitaria segura y de calidad.

El gobierno de las TIC es correcto cuando su gestión se encuentra alineada con los objetivos de negocio, se conocen los riesgos que afectan a los sistemas de información, y estos se gestionan adecuadamente. En este sentido, en una clara demostración de la importancia que la seguridad de la información tiene para el éxito de las organizaciones, la ISO y la IEC (International Electrotechnical Comisión, organización de ámbito mundial dedicada a la estandarización en el mercado de la electrónica y tecnologías relacionadas) han elaborado conjuntamente todo tipo de normas, estándares, guías y informes técnicos relacionados con las TIC y, más particularmente, con las técnicas de seguridad.

ISO/IEC ha reservado la familia de normas **ISO 27000** para tratar distintos aspectos de esta temática, del mismo modo que se ha realizado con la calidad y la familia ISO 9000, o la gestión medioambiental con la ISO 14000.

ISO/IEC 27001:2013. Es la norma que recoge los requerimientos para la implantación de un sistema de gestión de la seguridad de la información. La implantación de un SGSI según esta norma puede certificarse.

Por otro lado la **ISO/IEC 27002:2013** es el código de buenas prácticas para la gestión de la seguridad de la información, y recoge un completo y amplio catálogo de controles y buenas prácticas en la materia. Es el conjunto de controles que la Norma ISO/IEC 270001 toma como referencia a la hora de seleccionar controles de seguridad.

Por otra parte, la Norma **ISO/IEC 27799** - Gestión de la seguridad de la información en salud utilizando - Informática de la salud ISO / IEC 27002 proporciona orientación a las organizaciones sanitarias sobre la mejor manera de proteger la confidencialidad, integridad y disponibilidad de la información de salud mediante la implementación de la norma ISO / IEC 27002. En concreto, esta norma se ocupa de las necesidades de gestión de la seguridad de la información especial del sector de la salud y sus entornos operativos únicos.

Mientras que la protección y la seguridad de la información personal son importantes para todas las personas, empresas, instituciones y gobiernos, existen requisitos especiales en el sector de la salud que deben cumplirse para asegurar la confidencialidad, integridad, auditabilidad y la disponibilidad de información de salud. Este tipo de información es considerado por muchos como uno de los más confidenciales de todos los tipos de información personal. La protección de esta **confidencialidad** es esencial para mantener la privacidad de los sujetos de la atención sanitaria. La **integridad** de la información de salud debe ser protegida para garantizar la **seguridad del paciente**, y un componente importante de esa protección es garantizar que todo el ciclo de vida de la información sea completamente auditable. La **disponibilidad** de la información sobre la salud es también fundamental para una asistencia sanitaria eficaz. Los sistemas informáticos de salud deben cumplir con unas demandas únicas para seguir funcionando en caso de catástrofes naturales, fallos del sistema y ataques de denegación de servicio. La protección de la confidencialidad, integridad y disponibilidad de la información de salud, por lo tanto requiere de conocimientos específicos del sector de la salud.

Precisamente, la seguridad del paciente es uno de los aspectos que más preocupan a las organizaciones sanitarias, que no pueden entender la seguridad de la información sino es para proteger la salud de las personas. En línea con esta preocupación, y a modo de filtro, y con el objeto de cambiar la perspectiva de la seguridad de la información tratando de acentuar la importancia de los riesgos de las tecnologías de la información sanitarias en la salud de los pacientes, se tendrán muy en cuenta en este proyecto los aspectos considerados en las guías **SAFER (Safety Assurance Factors for EHR Resilience)** desarrolladas por la Office of the National Coordinator for Health Information Technology (ONC) de los EE.UU. Estas guías se enfocan en tres aspectos fundamentales: El diseño seguro de las Tecnologías de la Información de la Salud (TIS), El uso seguro de las TIS y la supervisión y monitorización continua de las TIS. En definitiva, es una visión de la seguridad en la que el paciente se convierte en el centro de la protección de las Tecnologías de la Información, tecnologías protegidas para proteger al paciente.

El planteamiento de este proyecto es por tanto, sentar las bases de un **Plan de Director de Seguridad para la organización** bajo esta visión. De manera simplificada, el proceso será el siguiente:

- Analizar y detallar nuestro inventario de activos.
- Estudiar las amenazas a las que están expuestos.
- Estudiar el impacto potencial de dichas amenazas.
- Proponer un plan de acción para luchar contra dichas amenazas.
- Evaluar el impacto residual una vez aplicado el plan de acción.

Intencionadamente, la lista anterior no contempla aspectos organizativos, que aún así, tocaremos a lo largo del presente proyecto.

2. Enfoque y selección de la empresa

Este proyecto se centrará en el Complejo Hospitalario Público Provincial que presta sus servicios sanitarios a una población de casi 800.000 habitantes.

2.1. Características del Hospital y actividad

El Complejo Público Hospitalario es un centro de asistencia sanitaria especializada, docencia e investigación en ciencias de la salud, integrado en el Sistema Sanitario Público. Su cartera de servicios abarca todas las áreas clínicas especializadas. Su actividad incluye procesos de máxima complejidad, así como una muy importante labor docente e investigadora. Su programa de trasplantes de órganos es líder a nivel nacional.

La plantilla del centro sanitario se compone de casi 5.000 trabajadores distribuidos según los siguientes grupos profesionales.

Grupo	Profesionales
Directivos	14
Facultativos	775
Facultativos en Formación	299
Diplomados Sanitarios	1.380
Diplomados Sanitarios en Formación	17
Técnicos especialistas	238
Auxiliares de Enfermería	994
Personal de Administración	499
Personal de Mantenimiento	104
Personal de hostelería y at. social	674
TOTAL	4.994

Tabla 1. Profesionales Complejo Hospitalario

En cuanto a su actividad asistencial los datos son los siguientes:

- **INGRESOS** 39.767
    1. Urgentes 17.819
    2. Programados 21.948
- **INTERVENCIONES** 39.820
    1. Programadas con ingreso 12.885
    2. Urgentes con Ingreso 3.938
    3. Cirugía Mayor Ambulatoria 10.878
    4. Resto Cirugía Ambulatoria 12.119

- **URGENCIAS ATENDIDAS** 193.979
    1. Adultos 126.959
    2. Pediatría 45.808
    3. Tocoginecología 21.215
- **CONSULTAS MEDICAS** 765.338
    1. Primeras Consultas 276.203
    2. Consultas Sucesivas 489.135
- **PARTOS** 2.912
- **CESAREAS** 733
- **ACTIVIDAD CONCERTADA**
    1. Resonancias Magnéticas 20
    2. Sesiones Hemodiálisis concert. 59.266
    3. Sesiones Diálisis Peritoneal conc. 8.672

2.2. Organigrama

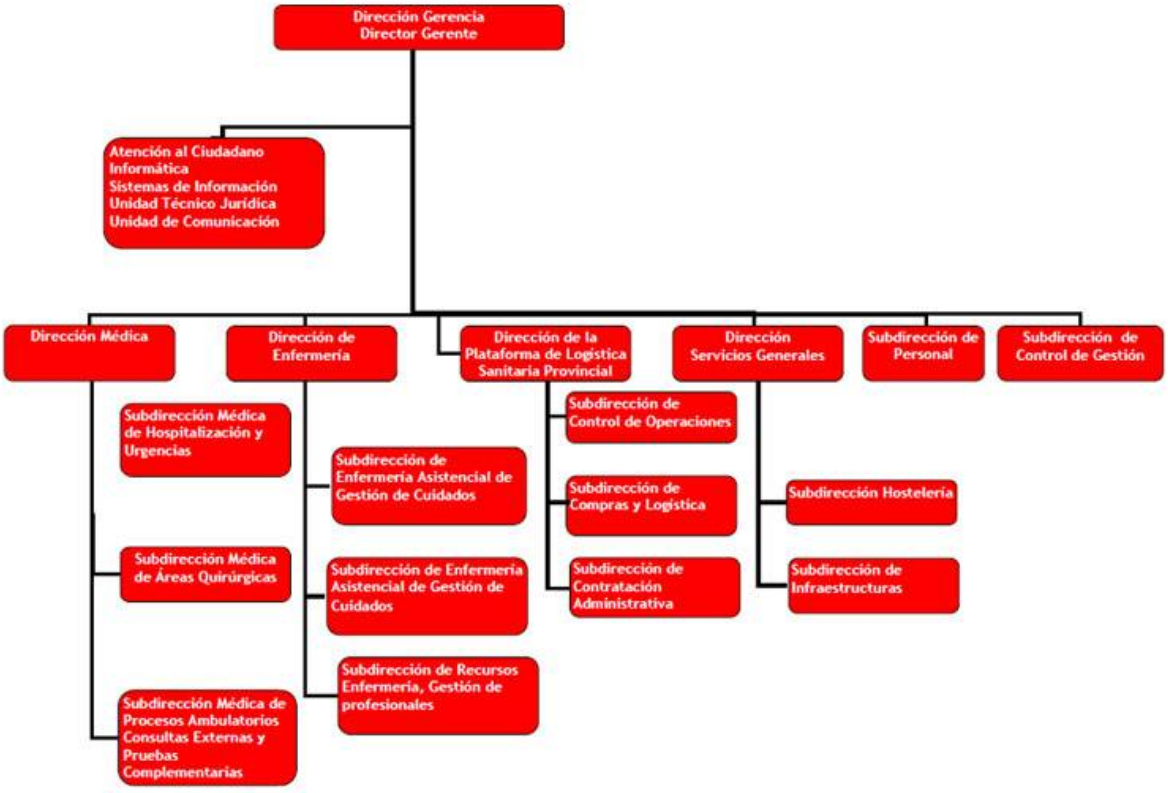


Ilustración 1. Organigrama del Complejo Hospitalario

La Dirección Gerencia dirige y coordina todas las actividades del centro hospitalario. Es el responsable último del centro y de este cargo dependen directamente los siguientes servicios:

- **Servicio de Atención al Ciudadano:** Atiende todas las dudas y trámites de cualquier paciente o ciudadano en relación con los servicios prestados por el centro hospitalario
- **Informática**: Servicio de soporte informático para todo el centro

- **Sistemas de Información:** Servicio de explotación y análisis de datos para la elaboración del cuadro de mandos del centro
- **Unidad Técnico Jurídica:** Asesoría jurídica a todo el equipo directivo
- **Unidad de Comunicación:** Gabinete de prensa del centro
- **Dirección Médica:** Dirección y coordinación de todos los servicios clínicos (Urgencias, Áreas Quirúrgicas, Consultas Externas y Pruebas complementarias y diagnósticas)
- **Dirección de Enfermería**: Dirección y coordinación de las actividades y profesionales de enfermería (Gestión de Cuidados y Gestión de profesionales)
- **Dirección de la plataforma logística sanitaria provincial**: Dirige y coordina los procesos de compra, almacenamiento y distribución de productos y artículos necesarios para la actividad diaria del centro sanitario.
- **Dirección de Servicios Generales**. Dirige y coordina las actividades de obras y mantenimiento de las infraestructuras del centro hospitalario
- **Subdirección de Personal**: Gestión de contratación y recursos humanos.
- **Subdirección de Control de Gestión**: Gestión de presupuestos y actividad económica del centro.

2.3. Medios

El complejo consta de 7 edificios dedicados a la asistencia sanitaria además de otros edificios dedicados al soporte para la asistencia, tales como cocinas, lavandería, investigación, archivos, edificios administrativos, etc.

- **Hospital General**. 58.702 m^2 en 8 plantas.
- **Edificio de Consultas Externas**. 16.404 m^2 en 6 plantas con un área dedicada a la docencia con 9 aulas, seminario, salón de actos, área de estudio y biblioteca.
- **Hospital Materno Infantil**. 17.748 m^2 en 8 plantas.
- **Hospital Provincial**. 32.583 m^2 en 13 plantas.
- **Hospital Salud Mental**. 17.062 m^2 en 8 plantas.
- **Centro de Especialidades Poniente**: 6.395,85 m^2 de superficie útil en 3 plantas
- **Centro de Diálisis**: 408 m^2 en planta baja.
- **Anatomía Patológica** (3.216 m2) en 2 plantas
- **Edificio de Gobierno**: 7.234 m^2. 3 plantas

Ilustración 2. Vista aérea del complejo hospitalario.

2.4. Equipamiento Informático

2.4.1. Estaciones de trabajo

El centro cuenta con unos 3.000 equipos (terminales e impresoras) para el acceso a los diversos sistemas de información del centro repartidos por todos los edificios y plantas del complejo hospitalario.

Todos los equipos conectan a través de red de datos de cableado estructurado mediante troncales de fibra entre los edificios y cableado estructurado de cobre entre las plantas de cada edificio

Se muestra a continuación un resumen del inventario del complejo hospitalario

Centro	Planta	Equipos PC	Equipos Impresion
Centro de Diálisis	1	22	2
Total Centro de Diálisis		22	2
Centro de Especialidades Poniente	1	15	2
	2	18	2
	3	34	3
Total Centro de Especialidades Poniente		67	7
Edificio Consultas Externas	1	71	7
	2	84	8
	3	79	8
	4	96	10
	5	84	8
	6	64	6
Total Edificio Consultas Externas		478	48
Edificio de Gobierno	1	53	5
	2	48	5
	3	62	6
Total Edificio de Gobierno		163	16
Hospital General.	1	163	36

	2	43	4
	3	40	4
	4	38	4
	5	45	5
	6	56	6
	7	68	7
	8	72	7
Total Hospital General.		525	72
Hospital Materno Infantil.	1	63	6
	2	82	8
	3	65	7
	4	76	8
	5	74	7
	6	54	5
	7	53	5
	8	53	5
Total Hospital Materno Infantil.		520	52
Hospital Provincial.	1	46	5
	2	55	6
	3	63	6
	4	65	7
	5	70	7
	6	68	7
	7	72	7
	8	82	8
	9	66	7
	10	73	7
	11	72	7
	12	67	7
	13	54	5
Total Hospital Provincial.		853	85
Hospital Salud Mental	1	24	2
	2	32	3
	3	25	3
	4	37	4
	5	28	3
	6	22	2
	7	34	3
	8	23	2
Total Hospital Salud Mental		225	23
Total general		2853	305

Tabla 2. Distribución de Equipamiento

2.4.2. Centros de Proceso de Datos

Se muestra a continuación un esquema básico del Centro de Proceso de datos del complejo hospitalario:

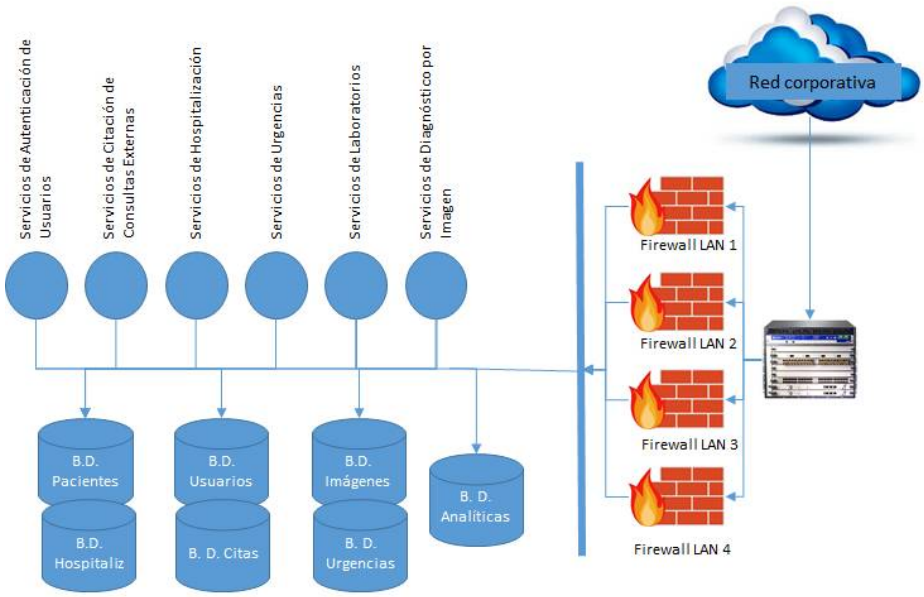


Ilustración 3. Centro de Proceso de Datos Local

El CPD local del centro hospitalario actua como respaldo local de otro CPD corporativo que da servicio a todo el servicio sanitario público. A su vez, este CPD corporativo está respaldado con un segundo CPD ubicado a 200 km del mismo. A diferencia de los otros dos CPD, el CPD local sólo mantiene copia de los datos propios del centro hospitalario y sólo entra en funcionamiento en casos muy concretos, como son actualizaciones que obligan a la parada de los centros de procesos superiores corporativos (principal y secundario) o caídas en las comunicaciones que impiden el acceso a los centros de proceso de datos desde el hospital. Se muestra a continuación esquema simplificado.

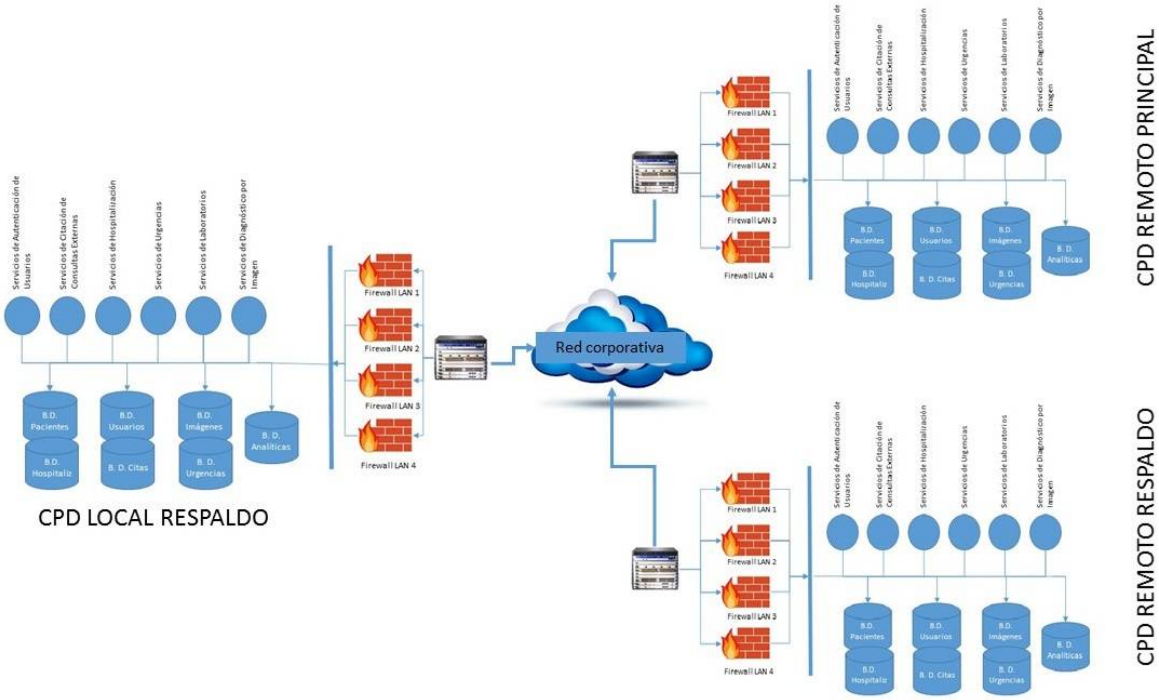


Ilustración 4. Centros de Proceso Principales y de Respaldo

2.4.3. Servidores Urgencias

Para dar servicio a la aplicación que soporta los procesos de urgencias se mantiene un armario rack de servidores y dos cabinas de discos tal y como muestra la figura siguiente:

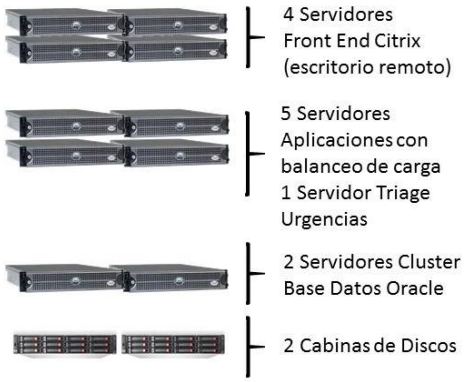


Ilustración 5. Distribución de Servidores de Urgencias

2.5. Comunicaciones

El núcleo de la red LAN del Hospital, se basa en un conmutador OmniSwitch OS-7700 con una procesadora (CMM), una placa de 12 puertos para MiniGBICs (que incluye varios 1000SX), y una placa de 12 puertos 10/100/1000.

Este equipo forma parte de una estrella conmutada conectada vía Gb sobre fibra (1000SX), que a su vez acaban en centros de otras "estrellas" de conmutación normalmente basadas en OmniSwitch-8008, de los que cuelgan diferentes pilas (hasta 19 en total), de OmniStacks-6148s, 6124s, 6024s o combinaciones de los mismos.

En el esquema siguiente, puede verse un dibujo de la red

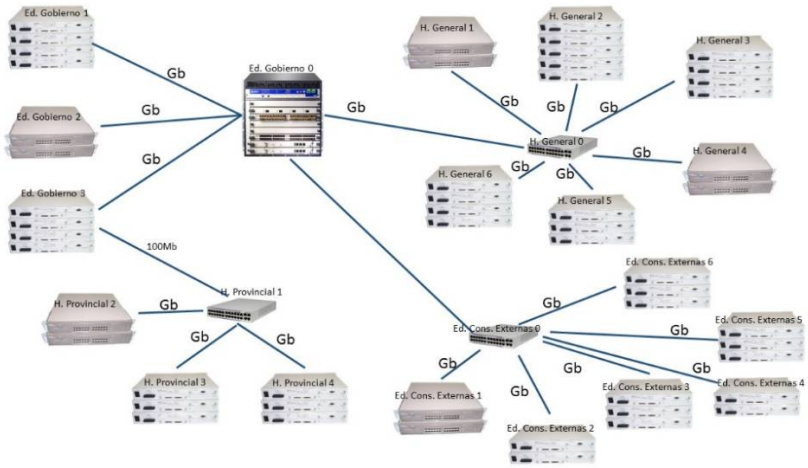


Ilustración 6. Red de Comunicaciones LAN

Por otro lado, esta red (intranet) conecta a la Red Corporativa de la Junta de Andalucía para dar acceso a los servicios centralizados corporativos.

2.6. Sistemas de Información

El mapa de procesos del complejo hospitalario es el siguiente:

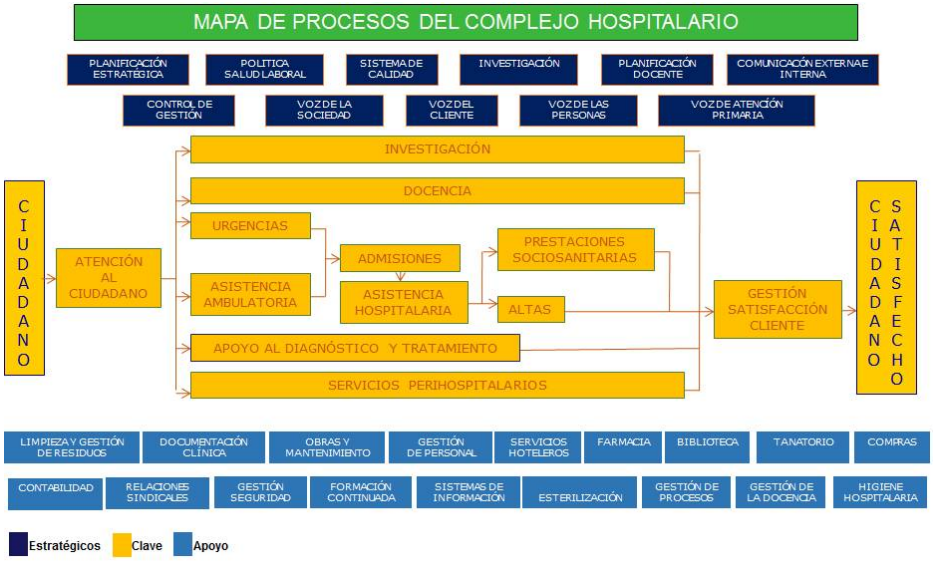


Ilustración 7. Mapa de Procesos del Complejo Hospitalario

Los sistemas de información con los que cuenta el complejo para cubrir estos procesos son los siguientes:

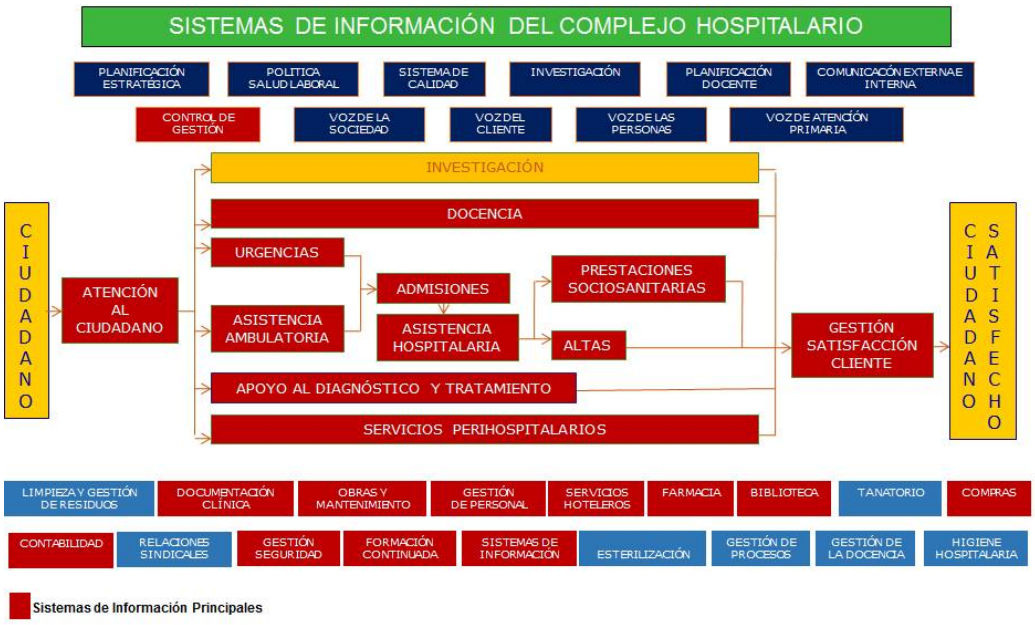


Ilustración 8. Cobertura de procesos informatizados

2.7. Alcance

El alcance del Sistema de este plan director para la Gestión de Seguridad de la Información se plantea para el proceso de Urgencias del complejo hospitalario. Proceso considerado **clave** en la prestación de la atención sanitaria de los pacientes que necesitan ser atendidos con mayor rápidez en un entorno de trabajo 24x7, 365 dias al año. El alcance concreto de este plan queda definido por la siguiente declaración:

Gestión de la Seguridad de la Información del proceso de urgencias incluyendo exclusivamente el **proceso de admisión de pacientes, clasificación de pacientes, seguimiento de pacientes en observación, registro de la atención sanitaria, petición electrónica de pruebas de laboratorio, petición electrónica de pruebas radiológicas y alta del paciente.** Este alcance está limitado por los procesos internos mencionados. Este alcance no contempla otros procesos externos correspondientes a otras servicios de apoyo al diagnóstico y tratamiento no relacionados directamente con el proceso de urgencias, tales como petición electrónica de estudios anatomopatológicos, de medicina nuclear ni de farmacia ni tampoco los procesos relacionados con los procesos de admisión, Hospitalización o citación y seguimiento de consultas externas ni planes de cuidados de enfermería. Todo esto de acuerdo con la declaración de aplicabilidad versión 1.0.

Dentro de los procesos del hospital este plan director se centra en el **PROCESO DE URGENCIAS.** La figura siguiente muestra este alcance en el contexto de los procesos generales del complejo hospitalario.

Ilustración 9. Alcance dentro del Mapa de Procesos del Complejo Hospitalario

Dentro del mapa de procesos general del hospital tenemos el mapa de procesos propio del servicio de atención en urgencias

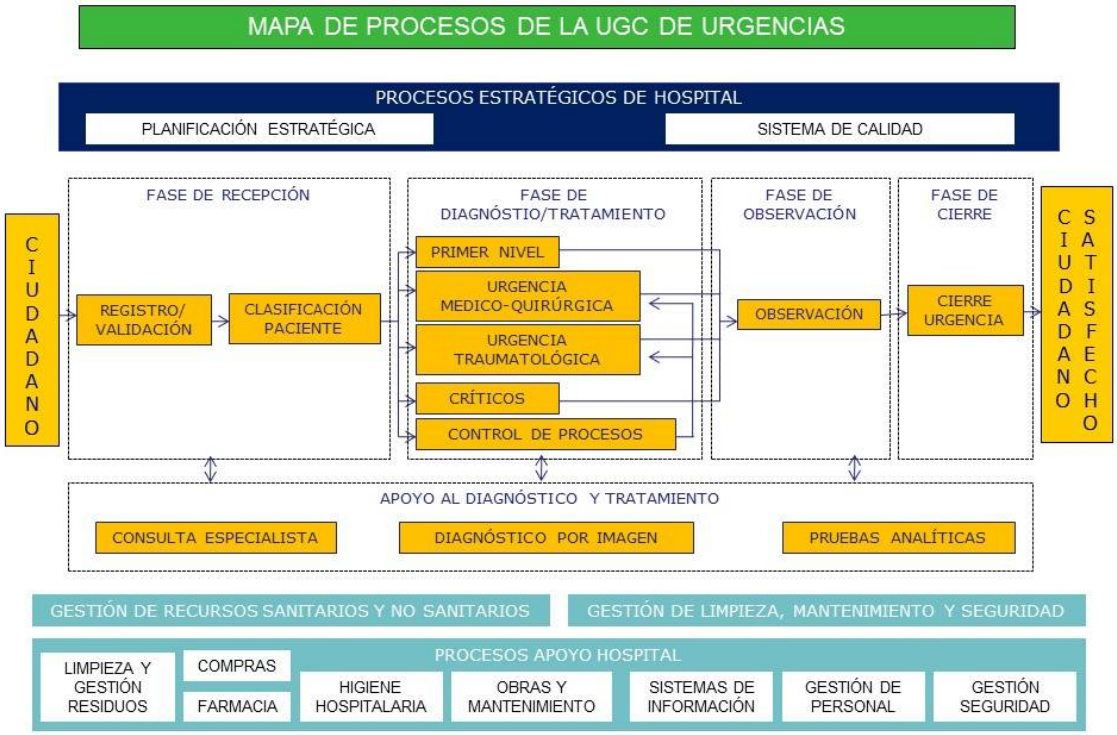


Ilustración 10. Mapa de Procesos de Urgencias

Se excluyen del alcance de este proyecto otros servicios como servicios web, correo electrónico, gestores documentales o cualquier otro servicio prestado al usuario no incluido en el mapa de procesos de la atención de urgencias.

3. Definición de Objetivos del Plan Director de Seguridad

El servicio de Urgencias del Complejo Hospitalario atendió el último año 193.979 urgencias, es decir, más de 500 urgencias diarias en un entorno de funcionamiento de 24x7 y 365 días al año. La cada vez mayor dependencia de los profesionales clínicos de las herramientas facilitadas por las Tecnologías de la Información Sanitarias obligan a tomar en serio la seguridad de los sistemas de información y los sistemas informáticos para poder garantizar los derechos de los ciudadanos a una asistencia sanitaria de calidad y eficiente.

El presente Plan Director de Seguridad persigue los siguientes objetivos:

- Asegurar la prestación de los servicios de atención en urgencias en régimen 24x7. Continuidad de Negocio
- Garantizar el cumplimiento legal establecido por la Ley Orgánica de Protección de Datos y legislación sanitaria relacionada.
- Asegurar la integridad de los datos de salud para una prestación de la atención sanitaria en urgencias segura para el paciente (libre de errores médicos debido a falta de información o información errónea)

- Identificar las necesidades organizativas respecto de la consecución de los objetivos anteriores.
- Poner en marcha el plan de mejora continua establecido por la norma ISO/IEC 27001

4. Análisis diferencial del sistema de urgencias respecto de la ISO/IEC 27001

Para la consecución de estos objetivos se contrastará la situación actual de la organización respecto de la norma ISO/IEC 27001 e ISO/IEC 27002 teniendo en cuenta además las recomendaciones de la ISO/IEC 27799 (International Standard ISO/IEC 27799. Gestión de la seguridad de la información en salud utilizando - Informática de la salud ISO / IEC 27002)

En este apartado realizamos el análisis diferencial sobre el estado de la situación actual respecto del cumplimiento de la norma ISO/IEC 27001

Esta Norma ha sido elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación del sistema de gestión de la seguridad de la información de una organización están influenciados por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales empleados, y el tamaño y estructura de la organización.

El sistema de gestión de la seguridad de la información preserva la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo, y brinda confianza a las partes interesadas acerca de que los riesgos son gestionados adecuadamente.

Es importante que el sistema de gestión de la seguridad de la información sea parte de los procesos y de la estructura de gestión total de la información de la organización y que esté integrado con ellos, y que la seguridad de la información se considere en el diseño de procesos, sistemas de información y controles.

Para elaborar el análisis diferencial hemos tenido en cuenta el modelo de madurez de la capacidad de los procesos de la norma ISO/IEC 15504. Se muestra a continuación la escala de madurez utilizada para la evaluación del cumplimiento de cada uno de los controles establecidos por la norma ISO/IEC 27001

Valor	Efectividad	Significado	Descripción
L0	0%	Proceso incompleto	El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.
L1	10%	Proceso Ejecutado	El proceso implementado alcanza su propósito
L2	50%	Proceso Gestionado	El proceso ejecutado descrito anteriormente está ya implementado de forma gestionada (planificado, supervisado y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.

Valor	Efectividad	Significado	Descripción		
L3	90%	Proceso Establecido	El proceso gestionado descrito anteriormente está ahora implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso. La implantación de los procesos se ha estandarizado (se documenta, se comunica y se da formación)		
L4	95%	Proceso Predecible	El proceso establecido descrito anteriormente ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.		
L5	100%	Proceso Optimizado	El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con las metas presentes y futuras.		
L6	N/A	No aplica			

Tabla 3. Modelo de evaluación de procesos ISO/IEC 15504.

Aunque tecnológicamente hablando el complejo hospitalario cuenta con numerosas medidas de seguridad (servidores duplicados, comunicaciones duplicadas, almacenamiento duplicados....) y la dirección está sensibilizada con la seguridad de la información en sus aspectos de protección de la confidencialidad y cuenta con políticas e infraestructuras organizativas para la toma de decisiones respecto de la seguridad de la información, en realidad, todo se ha ido construyendo a lo largo del tiempo a demanda de las directivas sanitarias o requerimientos legales exigibles. En definitiva, el complejo hospitalario no cuenta con un Sistema de Gestión de Seguridad de la Información y nunca se ha hecho un plan director de seguridad de la información más allá de iniciativas ad-hoc según las necesidades del momento y los presupuestos disponibles.

De acuerdo a los niveles de madurez mostrados en la figura anterior y los controles establecidos por la norma ISO/IEC 27001, el análisis diferencial arroja los siguientes resultados:

	Dominio	% de conformidad	# No Conformidades mayores	# No Conformidades menores	# Conformidades OK
4	**Contexto de la organización**	29%	4	0	1
5	**Liderazgo**	17%	13	1	3
6	**Planificación**	0%	32	0	0
7	**Soporte**	20%	23	3	0
8	**Operación**	0%	9	0	0
9	**Evaluación del Rendimiento**	0%	23	0	0
10	**Proceso de mejora**	0%	11	0	0

Tabla 4. Resultados Análisis Diferencial ISO/IEC 27001

Se muestra a continuación resumen gráfico de conformidad con la norma ISO/IEC 27001

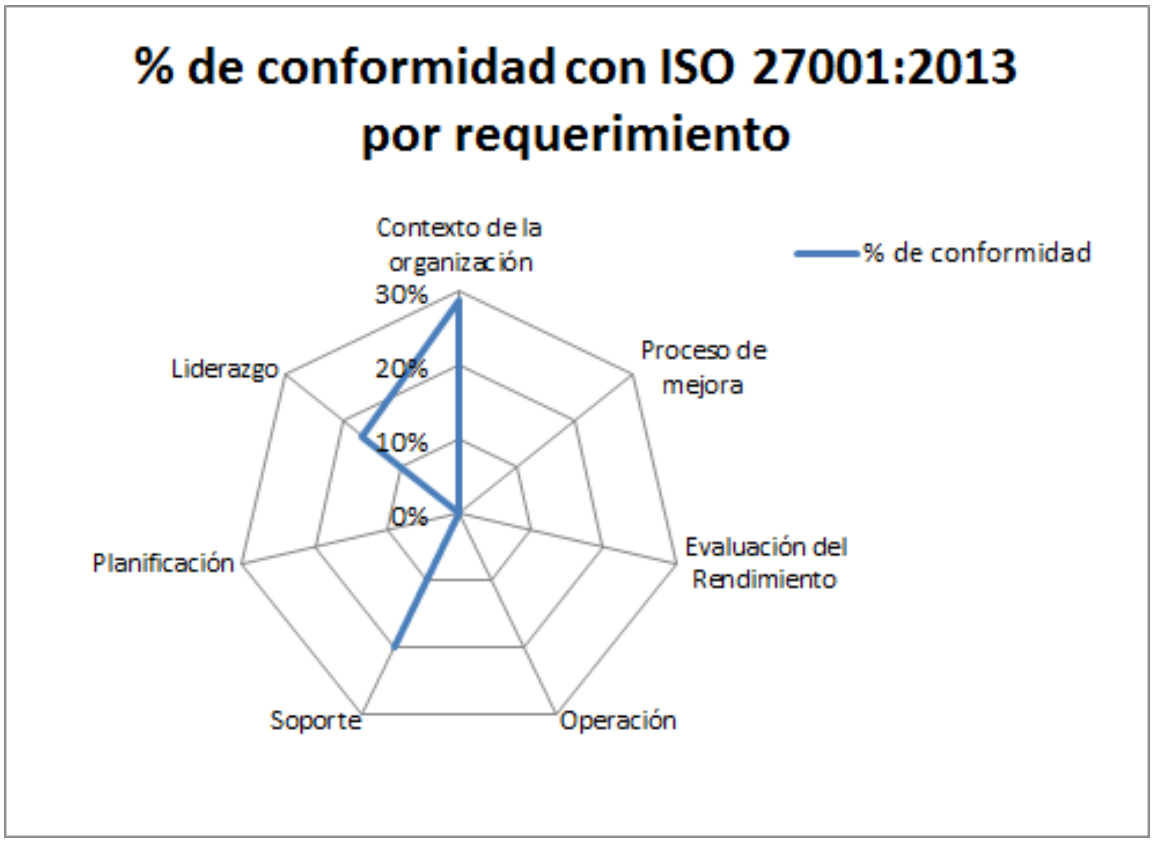


Ilustración 11. Gráfico Resultados Análisis Diferencial ISO/IEC 27001

En cuanto a la clasificación de los controles por nivel de madurez, podemos observar la siguiente figura:

Valor	Efectividad	Significado	Descripción	Número
L0	0%	Proceso incompleto	El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.	106
L1	10%	Proceso Ejecutado	El proceso implementado alcanza su propósito	9
L2	50%	Proceso Gestionado	El proceso ejecutado descrito anteriormente está ya implementado de forma gestionada (planificado, supervisado y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.	1
L3	90%	Proceso Establecido	El proceso gestionado descrito anteriormente está ahora implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso. La implantación de los procesos se ha estandarizado (se documenta, se comunica y se da formación)	3
L4	95%	Proceso Predecible	El proceso establecido descrito anteriormente ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.	3
L5	100%	Proceso Optimizado	El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con las metas presentes y futuras.	1
L6	N/A	No aplica		0

Tabla 5. Modelo Evaluación Madurez ISO/IEC 15504

El *Anexo I - Análisis diferencial detallado del sistema de urgencias respecto de la ISO/IEC 27001* contiene todos los detalles del análisis

5. Análisis diferencial del sistema de urgencias respecto de la ISO/IEC 27002

En este apartado se realiza un análisis diferencial de la situación actual de los controles de seguridad establecidos por la norma ISO 27002:2013. Este análisis establece el punto de partida tomado como referencia para evaluar el avance del plan director.

Igual que para el análisis realizado en el apartado anterior, la evaluación los controles para cada uno de los dominios se han obtenido calculando el promedio de la efectividad de los controles de cada uno de los dominios.

Para la valoración de cada uno de los controles de la norma 27002 se han tenido en cuenta las recomendaciones establecidas en ISO/IEC 27799 (International Standard ISO/IEC 27799. Gestión de la seguridad de la información en salud utilizando - Informática de la salud ISO / IEC 27002)

Los resultados obtenidos en este primer análisis arrojan los siguientes resultados:

Dominio		% de conformidad	# NC baja efectividad	# NC alta efectividad	# NC OK
A.5	POLÍTICAS DE SEGURIDAD	10%	2	0	0
A.6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.	29%	6	0	1
A.7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	42%	2	2	1
A.8	GESTIÓN DE ACTIVOS.	15%	9	1	0
A.9	CONTROL DE ACCESOS.	8%	14	0	0
A.10	CIFRADO.	10%	2	0	0
A.11	SEGURIDAD FÍSICA Y AMBIENTAL.	31%	7	8	0
A.12	SEGURIDAD EN LA OPERATIVA.	8%	14	0	0
A.13	SEGURIDAD EN LAS TELECOMUNICACIONES.	23%	5	2	0
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	12%	12	1	0
A.15	RELACIONES CON SUMINISTRADORES.	4%	5	0	0
A.16	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	1%	7	0	0
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	5%	4	0	0
A.18	CUMPLIMIENTO.	25%	4	4	0

Tabla 6. % de Conformidad con los Dominios ISO/IEC 27002

Se muestra a continuación gráfico de radar representando los porcentajes de cumplimientos por cada dominio ISO/IEC 27002.

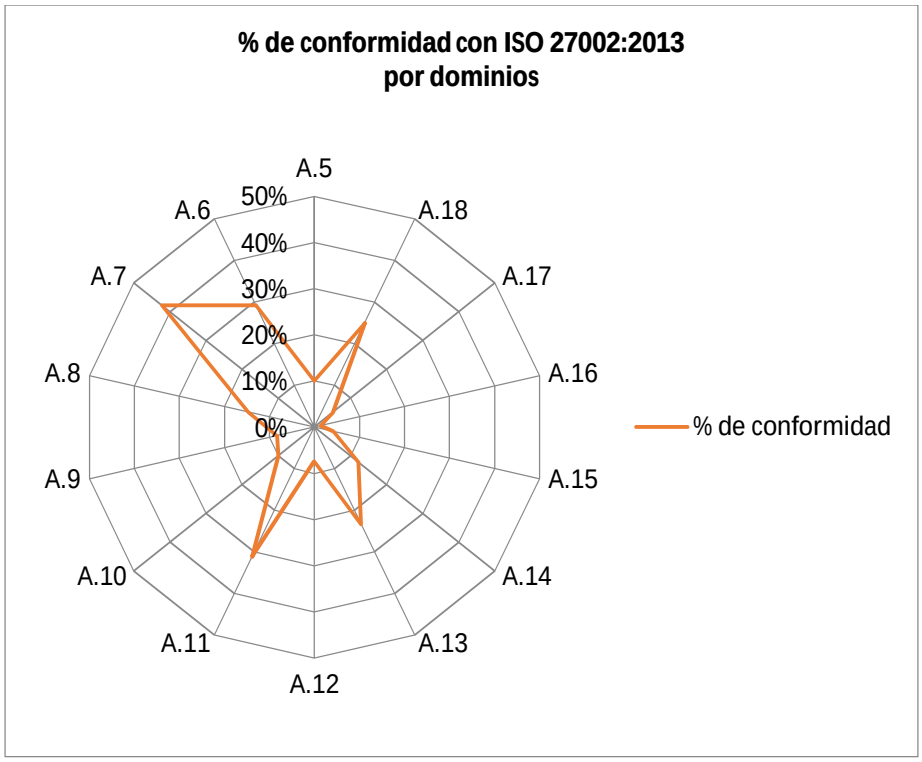


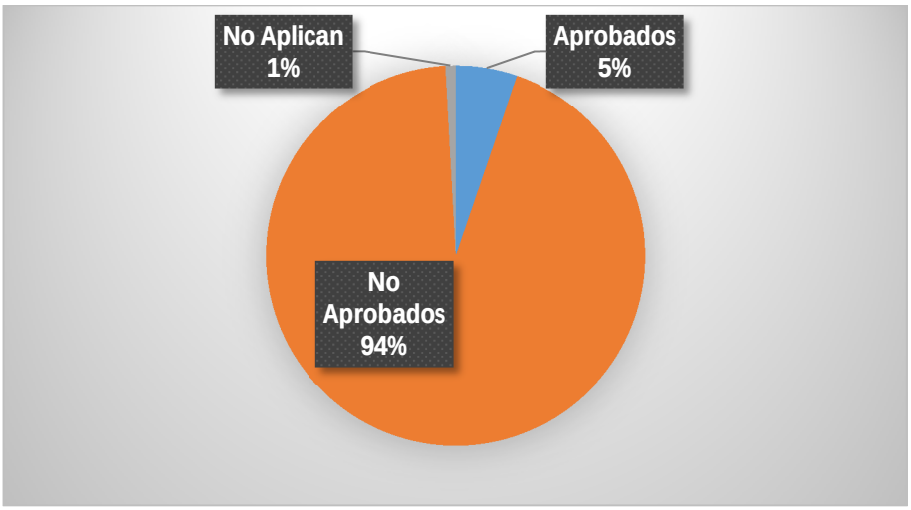
Ilustración 12. % de conformidad con ISO 27002:2013

Por niveles de madurez de la capacidad de los procesos hemos obtenido lo siguiente:

Valor	Efectividad	Significado	Descripción	Número
L0	0%	Proceso incompleto	El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.	32
L1	10%	Proceso Ejecutado	El proceso implementado alcanza su propósito	61
L2	50%	Proceso Gestionado	El proceso ejecutado descrito anteriormente está ya implementado de forma gestionada (planificado, supervisado y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.	14
L3	90%	Proceso Establecido	El proceso gestionado descrito anteriormente está ahora implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso. La implantación de los procesos se ha estandarizado (se documenta, se comunica y se da formación)	4
L4	95%	Proceso Predecible	El proceso establecido descrito anteriormente ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.	2
L5	100%	Proceso Optimizado	El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con las metas presentes y futuras.	0
L6	N/A	No aplica		1

Tabla 7. Número de Controles por Nivel de Madurez del proceso.

Por último, la siguiente figura muestra los mismos datos en gráfico circular en porcentajes.



El *Anexo II - Análisis diferencial detallado del sistema de urgencias respecto de la ISO/IEC 27002* contiene todos los detalles del análisis

Fase 2. Sistema De Gestión Documental

Todos los Sistemas de Gestión se apoyan en un cuerpo documental para el cumplimiento normativo. Esto significa que en nuestro Sistema de Gestión de Seguridad de la Información tendremos que tener una serie de documentos, los cuales vienen establecidos en la propia norma ISO/IEC 27001

1. Introducción

Todos los Sistemas de Gestión se apoyan en un cuerpo documental para el cumplimiento normativo. Esto significa que en nuestro Sistema de Gestión de Seguridad de la Información tendremos que tener una serie de documentos, los cuales vienen establecidos en la propia norma ISO/IEC 27001

Con el esquema documental básico que establece la norma preparado, tendremos establecidas las bases de nuestro Sistema de Gestión de Seguridad de la Información, ya que sobre estos documentos y/o políticas/procedimientos se llevarán a cabo las diferentes actividades de implantación (realización del análisis de riesgos, implantación de controles necesarios, implantación de proyectos, realización de auditoría interna, etc).

2. Esquema Documental

La propia ISO/IEC 27001 define cuales son los documentos necesarios para poder certificar el sistema, nos centraremos en los siguientes:

- Política de Seguridad
- Procedimiento de Auditorías Internas
- Gestión de Indicadores
- Procedimiento de Revisión por la Dirección
- Gestión de Roles y Responsabilidades
- Metodología de Análisis de Riesgos
- Declaración de Aplicabilidad

La existencia de todos estos documentos constituyen evidencias palpables de que el Sistema de Gestión está funcionando. En los siguientes apartados se detallan dichos documentos.

2.1. Política de Seguridad

La política de seguridad constituye la normativa interna que debe conocer y cumplir todo el personal afectado por el alcance del Sistema de Gestión de Seguridad de la Información. El contenido de la Política debe cubrir aspectos relativos al acceso de la información, uso de recursos de la Organización, comportamiento en caso de incidentes de seguridad, etc.

El anexo III recoge un resumen del documento de políticas de la seguridad de la información. Se puede ver el documento completo en ***01 - 01 DocumentoPolíticasSeguridad.pdf***

2.2. Procedimiento de Auditorías Internas

Se trata del documento que debe incluir una planificación de las auditorías que se llevarán a cabo durante la vigencia del Sistema de Gestión de Seguridad de la Información. El Anexo III incluye un resumen del procedimiento establecido para este SGSI. Se puede ver el documento completo en el documento ***02 - 01 - ProcedimientoAuditoríaSGSI.pdf (POE - SGSI - 0201)***

2.3. Gestión de Indicadores

Es necesario definir indicadores para medir la eficacia de los controles de seguridad implantados. Igualmente es importante definir la sistemática para medir.

El procedimiento define los indicadores aplicables al Sistema de Gestión de Seguridad de la Información. El Anexo IV muestra los indicadores definidos. Puede encontrarse el documento completo en *03 - 01 - GestionIndicadores.pdf (**POE - SGSI - 0301)***

2.4. Procedimiento de Revisión por la Dirección

La Dirección de la Organización debe revisar anualmente las cuestiones más importantes que han sucedido en relación al Sistema de Gestión de Seguridad de la Información. Para esta revisión, la ISO/IEC 27001 define tanto los puntos de entrada, como los puntos de salida que se deben obtener de estas revisiones.

La revisión se llevará a cabo al menos una vez al año siendo la Comisión de Seguridad de la Información la encargada de la elaboración de los informes necesarios y el Responsable de Seguridad de la Información quién presente a la dirección sus resultados y conclusiones

El Anexo V contiene un breve resumen del procedimiento de revisión. El documento completo puede encontrarse en ***04 - 01 - ProcedimientoRevisionDireccion. pdf (POE - SGSI - 0401)***

2.5. Gestión de Roles y Responsabilidades

El Sistema de Gestión de Seguridad de la Información tiene que estar compuesto por un equipo que se encargue de crear, mantener, supervisar y mejorar el Sistema. Este equipo de trabajo, conocido habitualmente como Comité de Seguridad, debe estar compuesto al menos por una persona de Dirección, para que de esta manera las decisiones que se tomen puedan estar respaldadas por alguien de Dirección.

El Anexo VI muestra un breve resumen del diseño y funcionamiento del Comité de Seguridad de la Información. Se puede consultar el documento completo en 05 - 01 - Gestion de Roles y Responsabilidades. pdf (**POE - SGSI - 0501)**

2.6. Metodología de Análisis de Riesgos

La metodología de análisis de riesgos establece la sistemática que se seguirá para calcular el riesgo, lo cual deberá incluir básicamente la identificación y valoración de los activos, amenazas y vulnerabilidades. Se utlizará Magerit v3.0 como metodología de análisis de riesgos para este plan. Se trata de una metodología muy extendida y probada, que tiene la ventaja de expresar sus resultados en términos cuantitativos o cualitativos. Esto facilita la tarea a la hora de tomar decisiones y que estas decisiones sean a su vez validadas rápidamente por dirección.

En el **ANEXO VII** se incluye un breve resumen a la metodología Magerit v3.0. Se puede encontrar el documento completo en ***06 - 01 - ProcedimientoAnalisisYGestionRiesgos.pdf (POE - SGSI - 0601).***

Este procedimiento se completa con el procedimiento que define los criterios de aceptación del riesgo de la organización, ***06 - 02 - Criterios Aceptacion Riesgo. pdf (POE - SGSI - 0602)***

2.7. Declaración de Aplicabilidad

Es el documento que incluye todos los controles de Seguridad establecidos en la Organización, con el detalle de su aplicabilidad, estado y documentación relacionada.

El anexo VIII incluye la tabla correspondiente al Documento de Aplicabilidad del Sistema de Gestión de Seguridad de la Información, incluyendo los controles aplicables y no aplicables, razón de aplicabilidad, Procesos o documentos relacionas, indicardor asociado si lo hubiera y estado actual según el análisis diferencial realizado en la fase 1.

Se puede consultar el documento completo en ***07 - 01 - DeclaracionAplicabilidad (IN - SGSI - 0701)***

FASE 3: Análisis de Riesgos

1. Introducción

El Análisis de Riesgos es el proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización. Sabiendo lo que podría pasar, hay que tomar decisiones sobre el tratamiento del riesgo.

Hay múltiples formas de tratar un riesgo: evitar las circunstancias que lo provocan, reducir las posibilidades de que ocurra, acotar sus consecuencias, compartirlo con otra organización (por lo general contratando un servicio o un seguro de cobertura), o, en última instancia, aceptando que pudiera ocurrir y previendo recursos para actuar cuando sea necesario.

Es también una opción legítima aceptar el riesgo. Aunque es frecuente oír que la seguridad absoluta no existe, siempre hay que aceptar un riesgo que, eso sí, debe ser conocido y sometido al umbral de calidad que se requiere del servicio. Es más, a veces aceptamos riesgos operacionales para acometer actividades que pueden reportarnos un beneficio que supera al riesgo, o que tenemos la obligación de afrontar. Es por ello que a veces se emplean definiciones más amplias de riesgo:

Efecto de la incertidumbre sobre la consecución de los objetivos [ISO Guía 73]

Como todo esto es muy delicado, no es meramente técnico, e incluye la decisión de aceptar un cierto nivel de riesgo, deviene imprescindible saber en qué condiciones se trabaja y así poder ajustar la confianza que merece el sistema. Para ello, qué mejor que una aproximación metódica que permita tomar decisiones con fundamento y explicar racionalmente las decisiones tomadas.

El análisis de riesgos que sigue a continuación consta de las fases siguientes:

- Inventario de Activos
- Valoración de Activos
- Análisis de Amenazas
- Impacto y Riesgo Potencial
- Impacto y Riesgo Residual

2. Inventario de Activos

Un Activo se define como:

> Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE 71504:2008]

En un sistema de información hay 2 cosas esenciales:

- la información que maneja
- y los servicios que presta.

Para nuestro sistema de información hemos considerado los tipos activos siguientes, apoyándonos en el catálogo de activos de Magerit v.3. Libro II Catálogo de Elementos:

ACTIVO	DESCRIPCIÓN
AUX	Equipamiento Auxiliar
L	Instalaciones
P	Personal
HW	Hardware
SW	Software
COM	Comunicaciones
SI	Soportes de Información
D	Datos / Información
S	Servicios
O	Objetivos y Misión
IMG	Imagen, reputación, credibilidad
IND	Independencia de critero o actuación
KNW	Conocimeinto acumulado
IP	Intimidad / Honor de las personas
IF	Integridad Fisica de las personas

Tabla 8. Tipos de Activos

Se han clasificado estos tipos de activos según sus dependencias genéricas agrupándolos en 5 Capas concéntricas:

Codigo	Descripción	Explicación
C1	CAPA 1	Equipamientos básicos, Energía electrica, climatización, comunicaciones, personal de operaciones, mobiliario, edificios....
C2	CAPA 2	El sistema de Información, Equipos informáticos, hardware, software, aplicaciones, soportes de información...
C3	CAPA 3	La Información. Datos y Metadatos
C4	CAPA 4	Los Servicios. Objetivos, misión, bienes y servicios prestados
C5	CAPA 5	Otros Activos: Credibilidad, buena imagen, Conocimiento acumulado, independencia de criterio o actuación, Intimidad de las personas, Integridad física de las personas, Derechos de las personas

Tabla 9. Capas Concétricas de dependencias de los tipos de Activos

De esta forma, los tipos de activos, y por tanto los activos, quedan clasificados por capas de la forma siguiente:

CAPA	ACTIVO	DESCRIPCIÓN
C1	AUX	Equipamiento Auxiliar
C1	L	Instalaciones
C1	P	Personal
C2	HW	Hardware
C2	SW	Software
C2	COM	Comunicaciones
C2	SI	Soportes de Información
C3	D	Datos / Información
C4	S	Servicios
C4	O	Objetivos y Misión
C5	IMG	Imagen, reputación, credibilidad
C5	IND	Independencia de critero o actuación
C5	KNW	Conocimeinto acumulado
C5	IP	Intimidad / Honor de las personas
C5	IF	Integridad Fisica de las personas

Tabla 10. Clasificación de los Activos según las Capas de dependencias

Siguiendo estos criterios de clasificación y el catálogo de elementos de Magerit v3.0 se han identificado los siguientes activos dentro del alcance de este proyecto:

CAPA	TIPO	ACTIVO	DESCRIPCIÓN
C1	AUX	UPS	sistemas de alimentación ininterrumpida
C1	AUX	GEN	generadores eléctricos
C1	AUX	AC	equipos de climatización
C1	AUX	WIRE	cable eléctrico
C1	AUX	FIBER	fibra óptica
C1	AUX	SUPPLY	suministros esenciales
C1	AUX	FURNITURE	mobiliario: armarios, etc
C1	L	SITE	recinto
C1	L	CAR	Vehículo terrestre: ambulancias.
C1	L	PLANE	vehículo aéreo: avión y helicoptero
C1	COM	PSTN	red telefónica
C1	COM	LAN	red local
C1	COM	MAN	red metropolitana
C1	P	UI	usuarios internos
C1	P	OP	operadores
C1	P	ADM	administradores de sistemas
C1	P	COM	administradores de comunicaciones
C1	P	DBA	administradores de BBDD
C1	P	SUB	subcontratas
C2	HW	MID	equipos medios
C2	HW	PC	informática personal
C2	HW	BACKUP	equipamiento de respaldo

CAPA	TIPO	ACTIVO	DESCRIPCIÓN
C2	HW	PRINT	medios de impresión
C2	HW	SWITCH	conmutadores
C2	HW	BRIDGE	pasarelas
C2	HW	FIREWALL	cortafuegos
C2	MEDIA	SAN	almacenamiento en red
C2	S	DIR	servicio de directorio
C2	S	IDM	gestión de identidades
C2	S	IPM	gestión de privilegios
C2	SW	BROWSER	navegador web
C2	SW	WWW	servidor de presentación
C2	SW	APP	servidor de aplicaciones
C2	SW	DBMS	sistema de gestión de bases de datos
C2	SW	AV	anti virus
C2	SW	OS	sistema operativo
C2	SW	HYPERVISOR	gestor de máquinas virtuales
C2	SW	TS	servidor de terminales
C2	SW	BACKUP	sistema de backup
C3	D	PERA	Datos de carácter personal nivel alto
C3	D	BACKUP	Copias de respaldo
C3	D	CONF	Datos de configuración
C3	D	PASSWORD	Credenciales de usuario
C3	D	AUTH	datos de validación de credenciales
C3	D	ACL	datos de control de acceso
C3	D	LOG	registro de actividad
C3	D	EXE	código ejecutable
C3	D	TEST	datos de prueba
C4	O	O	Objetivos y Misión
C5	IMG	IMG	Imagen, reputación, credibilidad
C5	KNW	KNW	Conocimiento acumulado
C5	IP	IP	Intimidad / Honor de las personas
C5	IF	IF	Integridad Fisica de las personas

Tabla 11. Catálogo de Activos

3. Valoración de Activos

La valoración se puede ver desde la perspectiva de la "necesidad de proteger" pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes.

El valor nuclear suele estar en la información que el sistema maneja y los servicios que se prestan (activos denominados esenciales), quedando los demás activos subordinados a las necesidades de explotación y protección de lo esencial.

De un activo puede interesar calibrar diferentes dimensiones:

- su **confidencialidad:** ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.
- su **integridad**: ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.
- su **disponibilidad**: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios
- la **autenticidad**: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa? Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar)
- la **trazabilidad**: del servicio: ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo? Del acceso a los datos ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

Para este proyecto se ha adoptado una metodología de valoración cualitativa. Las escalas cualitativas permiten avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto de los demás. Es frecuente plantear estas escalas como órdenes de magnitud y, en consecuencia, derivar estimaciones del orden de magnitud del riesgo. La limitación de las valoraciones cualitativas es que no permiten comparar valores más allá de su orden relativo. No se pueden sumar valores.

La tabla siguiente nos ha ayudado a llevar a cabo la valoración de los activos de forma homogénea en función del perjuicio ocasionado al activo en cada una de las dimensiones consideradas:

codigo	Perjucio al activo	descripcion
1	0	no afectaría a la seguridad de las personas
2	0	sería causa de inconveniencias mínimas a las partes afectadas
3	0	supondría pérdidas económicas mínimas
4	0	no supondría daño a la reputación o buena imagen de las personas u organizaciones
1da	1	Pudiera causar la interrupción de actividades propias de la Organización
1adm	1	Administración y gestión: pudiera impedir la operación efectiva de una parte de la organización
1lg	1	Pudiera causar una pérdida menor de la confianza dentro de la Organización

codigo	Perjucio al activo	descripcion
1olm	1	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
1iio	1	Pudiera causar algún daño menor a misiones importantes de inteligencia o información
1cei	1	Intereses comerciales o económicos:
1cei.a	1	de pequeño interés para la competencia
1cei.b	1	de pequeño valor comercial
1pi1	1	Información personal: pudiera causar molestias a un individuo
1lro	1	Obligaciones legales: pudiera causar el incumplimiento leve o técnico de una ley o regulación
1si	1	Seguridad: pudiera causar una merma en la seguridad o dificular la investigación de un incidente
1ps	1	Seguridad de las personas: pudiera causar daños menores a un individuo
1po	1	Orden público: pudiera causar protestas puntuales
1ir	1	Pudiera tener un impacto leve en las relaciones internacionales
1lbl	1	Datos clasificados como sin clasificar
2lg	2	Probablemente cause una pérdida menor de la confianza dentro de la Organización
2cei	2	Intereses comerciales o económicos:
2cei.a	2	de bajo interés para la competencia
2cei.b	2	de bajo valor comercial
2pi1	2	Información personal: pudiera causar molestias a un individuo
2pi2	2	Información personal: pudiera quebrantar de forma leve leyes o regulaciones
2ps	2	Seguridad de las personas: pudiera causar daño menor a varios individuos
2lbl	2	Datos clasificados como sin clasificar
3da	3	Probablemente cause la interrupción de actividades propias de la Organización
3adm	3	Administración y gestión: probablemente impediría la operación efectiva de una parte de la organización
3lg	3	Probablemente afecte negativamente a las relaciones internas de la Organización
3olm	3	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
3iio	3	Probablemente cause algún daño menor a misiones importantes de inteligencia o información
3cei	3	Intereses comerciales o económicos:
3cei.a	3	de cierto interés para la competencia
3cei.b	3	de cierto valor comercial
3cei.c	3	causa de pérdidas financieras o merma de ingresos
3cei.d	3	facilita ventajas desproporcionadas a individuos u organizaciones
3cei.e	3	constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
3pi1	3	Información personal: probablemente afecte a un individuo
3pi2	3	Información personal: probablemente suponga el incumplimiento de una ley o regulación
3lro	3	Obligaciones legales: probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
3si	3	Seguridad: probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente

codigo	Perjucio al activo	descripcion
3ps	3	Seguridad de las personas: probablemente cause daños menores a un individuo
3po	3	Orden público: causa de protestas puntuales
3ir	3	Probablemente cause un impacto leve en las relaciones internacionales
3lbl	3	Datos clasificados como de difusión limitada
4pi1	4	Información personal: probablemente afecte a un grupo de individuos
4pi2	4	Información personal: probablemente quebrante leyes o regulaciones
4ps	4	Seguridad de las personas: probablemente cause daños menores a varios individuos
4crm	4	Dificulte la investigación o facilite la comisión de delitos
4lbl	4	Datos clasificados como de difusión limitada
5da	5	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
5adm	5	Administración y gestión: probablemente impediría la operación efectiva de más de una parte de la organización
5lg	5	Probablemente sea causa una cierta publicidad negativa
5lg.a	5	por afectar negativamente a las relaciones con otras organizaciones
5lg.b	5	por afectar negativamente a las relaciones con el público
5olm	5	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
5iio	5	Probablemente dañe a misiones importantes de inteligencia o información
5pi1	5	Información personal: probablemente afecte gravemente a un individuo
5pi2	5	Información personal: probablemente quebrante seriamente leyes o regulaciones
5lro	5	Obligaciones legales: probablemente sea causa de incumplimiento de una ley o regulación
5ir	5	Probablemente tenga impacto en las relaciones internacionales
5lbl	5	Datos clasificados como de difusión limitada
6pi1	6	Información personal: probablemente afecte gravemente a un grupo de individuos
6pi2	6	Información personal: probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
6ps	6	Seguridad de las personas: probablemente cause daños de cierta consideración, restringidos a un individuo
6po	6	Orden público: probablemente cause manifestaciones, o presiones significativas
6lbl	6	Datos clasificados como de difusión limitada
7da	7	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
7adm	7	Administración y gestión: probablemente impediría la operación efectiva de la organización
7lg	7	Probablemente causaría una publicidad negativa generalizada
7lg.a	7	por afectar gravemente a las relaciones con otras organizaciones
7lg.b	7	por afectar gravemente a las relaciones con el público en general
7lg.c	7	por afectar gravemente a las relaciones con otros paises
7olm	7	Probablemente cause perjudique la eficacia o seguridad de la misión operativa o logística

codigo	Perjucio al activo	descripcion
7iio	7	Probablemente cause serios daños a misiones importantes de inteligencia o información
7cei	7	Intereses comerciales o económicos:
7cei.a	7	de alto interés para la competencia
7cei.b	7	de elevado valor comercial
7cei.c	7	causa de graves pérdidas económicas
7cei.d	7	proporciona ganancias o ventajas desmedidas a individuos u organizaciones
7cei.e	7	constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7lro	7	Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación
7si	7	Seguridad: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
7ps	7	Seguridad de las personas: probablemente cause daños de cierta consideración a varios individuos
7ir	7	Probablemente cause un impacto significativo en las relaciones internacionales
7lbl	7	Datos clasificados como confidenciales
8ps	8	Seguridad de las personas: probablemente cause daño a la seguridad o libertad individual (por ejemplo, es probable que llegue a amenazar la vida de uno o más individuos)
8crm	8	Impida la investigación de delitos graves o facilite su comisión
8lbl	8	Datos clasificados como confidenciales
9da	9	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
9adm	9	Administración y gestión: probablemente impediría seriamente la operación efectiva de la organización, pudiendo llegar a su cierre
9lg	9	Probablemente causaría causaría una publicidad negativa generalizada por por afectar de forma excepcionalmente grave a las relaciones ...
9lg.a	9	a las relaciones con otras organizaciones
9lg.b	9	a las relaciones con el público en general
9lg.c	9	a las relaciones con otros paises
9olm	9	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
9iio	9	Probablemente cause serios daños a misiones muy importantes de inteligencia o información
9cei	9	Intereses comerciales o económicos:
9cei.a	9	de enorme interés para la competencia
9cei.b	9	de muy elevado valor comercial
9cei.c	9	causa de pérdidas económicas excepcionalmente elevadas
9cei.d	9	causa de muy significativas ganancias o ventajas para individuos u organizaciones
9cei.e	9	constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
9lro	9	Obligaciones legales: probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
9si	9	Seguridad: probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
9ps	9	Seguridad de las personas: probablemente suponga la muerte de uno o más individuos

codigo	Perjucio al activo	descripcion
9po	9	Orden público: alteración seria del orden público
9ir	9	Probablemente cause un serio impacto en las relaciones internacionales
9lbl	9	Datos clasificados como reservados
10olm	10	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
10iio	10	Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información
10si	10	Seguridad: probablemente sea causa de un incidente excepcionalmente serior de seguridad o dificulte la investigación de incidentes excepcionalmente serios
10ps	10	Seguridad de las personas: probablemente suponga gran pérdida de vidas humanas
10po	10	Orden público: alteración seria del orden constitucional
10ir	10	Probablemente cause un impacto excepcionalmente grave en llas relaciones internacionales
10lbl	10	Datos clasificados como secretos

Tabla 12. Catálogo de Perjucios al Activo para su valoración

De acuerdo con el catálogo de activos de la tabla 11 y al catálogo de perjuicios de la tabla 12 se han valorado los activos desde la perspectiva de las dimensiones de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (de servicios y de datos), obteniendo los resultados mostrados en la tabla 14.

Para cada activo y por cada una de las dimensiones consideradas se incluyen el posible perjucio a dicho activo. Cada perjuicio tiene asignado un valor de 0 a 10 según la tabla siguiente:

Perjucio al activo	Valor del Activo	Descripción	
0	MB	Despreciable	Irrelevante a efectos prácticos
1	B	Bajo	Daño menor a la organización
2	B	Bajo	Daño menor a la organización
3	B	Bajo	Daño menor a la organización
4	M	Medio	Daño importante a la organización
5	M	Medio	Daño importante a la organización
6	M	Medio	Daño importante a la organización
7	A	Alto	Daño grave a la organización
8	A	Alto	Daño grave a la organización
9	A	Alto	Daño grave a la organización
10	MA	Muy Alto	daño muy grave a la organización

Tabla 13. Cáculo de la Valoración del Activo en función del perjuicio ocasionado

La columna **Valor Activo,** contiene el promedio del perjuicio calculado a partir de las columnas **Valor I, Valor C, Valor D, Valor A, Valor T** cuyos valores se derivan a su vez de los perjuicios incluidos en las columnas **I**, **C, D, A** y **T** para cada uno de los activos relacionados.

La columna **Valor Q** indica el valor cualitativo calculado para cada activo. Pueden consultarse todos los cálculos realizados en la hoja de cálculo adjunta denominada ***Analisis de Riegos V0.2.xlsx***

				Perjuicio en Dimensiones					Valor Perjuicio en Dimensiones					Valor Promedio del Activo	
CAPA	TIPO	ACTIVO	DESCRIPCIÓN	I	C	D	A	T	Valor I	Valor C	Valor D	Valor A	Valor T	Valor Activo	Valor Q
C1	AUX	UPS	sistemas de alimentación ininterrumpida	1	1	1da	1	1	0	0	1	0	0	1	B
C1	AUX	GEN	generadores eléctricos	1	1	1da	1	1	0	0	1	0	0	1	B
C1	AUX	AC	equipos de climatización	1	1	3da	1	1	0	0	3	0	0	3	B
C1	AUX	WIRE	cable eléctrico	1	1	3da	1	1	0	0	3	0	0	3	B
C1	AUX	FIBER	fibra óptica	1	1	3da	1	1	0	0	3	0	0	3	B
C1	AUX	SUPPLY	suministros esenciales	1	1	3da	1	1	0	0	3	0	0	3	B
C1	AUX	FURNITURE	mobiliario: armarios, etc	1	1	1da	1	1	0	0	1	0	0	1	B
C1	L	SITE	recinto	1	1	3da	1	1	0	0	3	0	0	3	B
C1	L	CAR	Vehículo terrestre: ambulancias.	1	1	1da	1	1	0	0	1	0	0	1	B
C1	L	PLANE	Vehículo aéreo: avión y helicoptero	1	1	1da	1	1	0	0	1	0	0	1	B
C1	COM	PSTN	red telefónica	1	1	1da	1	1	0	0	1	0	0	1	B
C1	COM	LAN	red local	1	1	3da	1	1	0	0	3	0	0	3	B
C1	COM	MAN	red metropolitana	1	1	3da	1	1	0	0	3	0	0	3	B
C1	P	UI	usuarios internos	1	1	1da	1	3lro	0	0	1	0	3	2	B
C1	P	OP	operadores	1	1	1olm	1	3lro	0	0	1	0	3	2	B
C1	P	ADM	administradores de sistemas	1	1	3olm	1	3lro	0	0	3	0	3	3	B
C1	P	COM	administradores de comunicaciones	1	1	3olm	1	3lro	0	0	3	0	3	3	B
C1	P	DBA	administradores de BBDD	1	1	3olm	1	3lro	0	0	3	0	3	3	B
C1	P	SUB	subcontratas	1	1	1olm	1	3lro	0	0	1	0	3	2	B
C2	HW	MID	equipos medios	1	1	3olm	1	3lro	0	0	3	0	3	3	B

				Perjuicio en Dimensiones					Valor Perjuicio en Dimensiones					Valor Promedio del Activo	
CAPA	TIPO	ACTIVO	DESCRIPCIÓN	I	C	D	A	T	Valor I	Valor C	Valor D	Valor A	Valor T	Valor Activo	Valor Q
C2	HW	PC	informática personal	1	1	1olm	1	1olm	0	0	1	0	1	1	B
C2	HW	BACKUP	equipamiento de respaldo	1	1	1olm	1	3lro	0	0	1	0	3	2	B
C2	HW	PRINT	medios de impresión	1	1	3olm	1	1olm	0	0	3	0	1	2	B
C2	HW	SWITCH	conmutadores	1	1	7olm	1	3si	0	0	7	0	3	5	M
C2	HW	BRIDGE	pasarelas	1	1	3olm	1	3si	0	0	3	0	3	3	B
C2	HW	FIREWALL	cortafuegos	1	1	7olm	1	7lro	0	0	7	0	7	7	A
C2	MEDIA	SAN	almacenamiento en red	1	1	10olm	1	10si	0	0	10	0	10	10	MA
C2	S	DIR	servicio de directorio	1	1	3da	1	3si	0	0	3	0	3	3	B
C2	S	IDM	gestión de identidades	1	1	3da	1	3si	0	0	3	0	3	3	B
C2	S	IPM	gestión de privilegios	1	1	3da	1	3si	0	0	3	0	3	3	B
C2	SW	BROWSER	navegador web	1	1	1olm	1	3si	0	0	1	0	3	2	B
C2	SW	WWW	servidor de presentación	1	1	7olm	1	7adm	0	0	7	0	7	7	A
C2	SW	APP	servidor de aplicaciones	1	1	7olm	1	7adm	0	0	7	0	7	7	A
C2	SW	DBMS	sistema de gestión de bases de datos	1	1	7olm	1	7adm	0	0	7	0	7	7	A
C2	SW	AV	anti virus	1	1	1olm	1	3si	0	0	1	0	3	2	B
C2	SW	OS	sistema operativo	1	1	9olm	1	9lro	0	0	9	0	9	9	A
C2	SW	HYPERVISOR	gestor de máquinas virtuales	1	1	7olm	1	7lro	0	0	7	0	7	7	A
C2	SW	TS	servidor de terminales	1	1	9olm	1	9olm	0	0	9	0	9	9	A
C2	SW	BACKUP	sistema de backup	1	1	1olm	1	1lg	0	0	1	0	1	1	B
C3	D	PERA	Datos de carácter personal nivel alto	9lro	9lro	6pi1	6pi2	7ps	9	9	6	6	7	8	A

				Perjuicio en Dimensiones					Valor Perjuicio en Dimensiones					Valor Promedio del Activo	
CAPA	TIPO	ACTIVO	DESCRIPCIÓN	I	C	D	A	T	Valor I	Valor C	Valor D	Valor A	Valor T	Valor Activo	Valor Q
C3	D	BACKUP	Copias de respaldo	3pi2	6pi2	4pi2	4pi2	1lg	3	6	4	4	1	4	M
C3	D	CONF	Datos de configuración	3da	1	3da	1	1lg	3	0	3	0	1	3	B
C3	D	PASSWORD	Credenciales de usuario	3da	6pi1	3da	9lro	9lro	3	6	3	9	9	6	M
C3	D	AUTH	datos de validación de credenciales	3da	6pi1	3da	9lro	9lro	3	6	3	9	9	6	M
C3	D	ACL	datos de control de acceso	3da	6pi1	3da	9lro	9lro	3	6	3	9	9	6	M
C3	D	LOG	registro de actividad	7lro	9lro	5lro	5lro	9lro	7	9	5	5	9	7	A
C3	D	EXE	código ejecutable	3da	1	3da	1	2lg	3	0	3	0	2	3	B
C3	D	TEST	datos de prueba	1	1	1da	1	1	0	0	1	0	0	1	B
C4	O	O	Objetivos y Misión	1	1	1	9lg.b	9lg.b	0	0	0	9	9	9	A
C5	IMG	IMG	Imagen, reputación, credibilidad	1	1	1	9lg.b	9lg.b	0	0	0	9	9	9	A
C5	KNW	KNW	Conocimiento acumulado	1	1	1	7lg.b	7lg.b	0	0	0	7	7	7	A
C5	IP	IP	Intimidad / Honor de las personas	1	1	1	9lro	9lro	0	0	0	9	9	9	A
C5	IF	IF	Integridad Fisica de las personas	10ps	1	10ps	9lro	9ps	10	0	10	9	9	10	MA

Tabla 14. Valoración Cualitativa de Activos

4. Análisis de Amenazas

Una vez valorados los activos cualitativamente el siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son "cosas que ocurren". Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño.

Una Amenaza se define como:

> Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008]

De acuerdo con el capítulo 5 del Catálogo de Elementos del libro II de Magerit v.3 consideraremos las amenezas relacionadas en la tabla siguiente:

CODIGO	DESCRIPCIÓN	Origen
N.1	Fuego	DESASTRES NATURALES
N.2	Daños por agua	DESASTRES NATURALES
N.+	Otros desastres naturales	DESASTRES NATURALES
I.1	Fuego	DESASTRES INDUSTRIALES
I.2	Daños por agua	DESASTRES INDUSTRIALES
I.3	Contaminación Mecánica	DESASTRES INDUSTRIALES
I.4	Contaminación Electromagnética	DESASTRES INDUSTRIALES
I.5	Averia de origen Físico o Lógico	DESASTRES INDUSTRIALES
I.6	Corte de Suministro Electrico	DESASTRES INDUSTRIALES
I.7	Condiciones inadecuadas de temperatura y/o humedad	DESASTRES INDUSTRIALES
I.8	Fallo de servicios de comunicaciones	DESASTRES INDUSTRIALES
I.9	Interrupción de otros servicios y suministros esenciales	DESASTRES INDUSTRIALES
I.10	Degradación de los soportes de almacenamiento de la información	DESASTRES INDUSTRIALES
I.11	Emanaciones electromanéticas	DESASTRES INDUSTRIALES
I.+	Otros desastres Industriales	DESASTRES INDUSTRIALES
E.1	Errores de los usuarios	ERRORES
E.2	Errores del administrador	ERRORES
E.3	Errores de monitorización (log)	ERRORES
E.4	Errores de Configuración	ERRORES
E.7	Deficiencias en la organización	ERRORES
E.8	Difusión de software dañino	ERRORES
E.9	Errores de [re-]encamininamiento	ERRORES
E.10	Errores de secuencia	ERRORES
E.14	Escapes de información	ERRORES
E.15	Alteración de la información	ERRORES
E.16	Introducción de información incorrecta	ERRORES
E.17	Degradación de la Información	ERRORES
E.18	Destrucción de la información	ERRORES
E.19	Divulgación de la información	ERRORES

CODIGO	DESCRIPCIÓN	Origen
E.20	Vulnerabilidades de los programas (software)	ERRORES
E.21	Errores de mantenimiento / actualización de programas (software)	ERRORES
E.23	Errores de mantenimiento / actualización de equipos (hardware)	ERRORES
E.24	Caida del sistema por agotamiento de recursos	ERRORES
E.28	Indisponibilidad del personal	ERRORES
A.4	Manipulación de la configuración	ATAQUES
A.5	Suplantación de la identidad del usuario	ATAQUES
A.6	Abuso de privilegios de acceso	ATAQUES
A.7	Uso no previsto	ATAQUES
A.8	Difusión de software dañino	ATAQUES
A.9	[re-]encaminamiento de mensajes	ATAQUES
A.10	Alteración de secuencia	ATAQUES
A.11	Acceso no autorizado	ATAQUES
A.12	Analisis de trafico	ATAQUES
A.13	Repudio	ATAQUES
A.14	Interceptación de información (escucha)	ATAQUES
A.15	Modificación de la Información	ATAQUES
A.16	Introducción de información falsa	ATAQUES
A.17	Corrupción de la información	ATAQUES
A.18	Destrucción de la información	ATAQUES
A.19	Divulgación de la información	ATAQUES
A.22	Manipulación de los programas	ATAQUES
A.24	Denegación de Servicio	ATAQUES
A.25	Robo	ATAQUES
A.26	Ataque Destructivo	ATAQUES
A.27	Ocupación Enemiga	ATAQUES
A.28	Indisponibilidad del personal	ATAQUES
A.29	Extorsion	ATAQUES
A.30	Ingenieria social	ATAQUES

Tabla 15. Catálogo de Amenazas

Las amenazas potenciales a los activos ocasionan una cierta degradación en los mismos si llegan a producirse. Por otro lado estas se producen con una determinada frecuencia. Se trata de valores subjetivos asignados para cada amenaza basados en la experiencia del consultor sobre el entorno en el que se está desarrollando el plan director.

Se ha utilizado la siguiente escala de degradación de los activos:

% degradación	Desripción
1	1% Degradación despreciable
10	10% Degradación Baja
50	50% Degradación Media
100	100% Degradación total

Tabla 16. Degradación de un activo por una amenaza

En cuanto a las frecuencias de ocurrencia de las amenazas se ha utilizado la tabla siguiente:

ID	Descripción	Frecuencia
PF	Poco Frecuente	Cada varios años
FN	Frecuencia Normal	Anualmente
F	Frecuente	Mensualmente
MF	Muy Frecuente	Diariamente

Tabla 17. Frecuencia de Ocurrencia de Amenazas

5. Impacto Potencial y Riesgo Potencial

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la proba-bilidad de ocurrencia.

El riesgo crece con el impacto y con la probabilidad de ocurrencia de la amenaza. La tabla siguiente muestra el impacto potencial de una amenaza sobre un activo en función del valor del activo.

		Degradación			
Valor del Activo		1	10	50	100
MA	Muy Alto	M	A	MA	MA
A	Alto	M	M	A	A
M	Medio	B	B	M	M
B	Bajo	MB	MB	B	B
MB	Muy Bajo	MB	MB	MB	MB
		Impacto			

Tabla 18. Impacto Potencial en función del valor del activo y su degradación

La **tabla 18** muestra la escala utilizada para el cálculo del impacto potencial. Por ejemplo: para un valor de un activo **A** (alto) con una degradación **50** por una determinada amenaza obtendremos un **impacto A** (Alto).

Por otro lado, calculamos el riesgo potencial a partir del Impacto Potencial y la frecuencia de ocurrencia de cada amenaza.

Impacto Potencial	Frecuencia			
	Varios Años	Anual	Mensual	Diario
	1	2	3	4
	PF	FN	F	MF
MA	A	MA	MA	MA
A	M	A	MA	MA
M	B	M	A	MA
B	MB	B	M	A
MB	MB	MB	B	M
	Riesgo			

Tabla 19. Cálculo del Riesgo Potencial a partir del Impacto potencial y la frecuencia de amenaza

Por ejemplo, para un impacto potencial **M** (Medio) con una frecuencia de amenaza **F (Mensual)** obtendremos un **riesgo potencial A** (alto)

El **Anexo IX** relaciona para cada uno de los activos considerados las amenazas potenciales a las cuales puede estar sometido y el cálculo del Impacto Potencial y Riesgo Potencial. Pueden consultarse todos los cálculos realizados en la hoja de cálculo adjunta denominada ***Analisis de Riegos V0.2.xlsx***

6. Nivel de Riesgo Aceptable

Según lo establecido en el documento **POE-SGSI-0602-V.1.0 Criterios de Aceptación del Riesgo** la calificación de los riesgos es la siguiente:

1. es **crítico** en el sentido de que requiere atención urgente
2. es **grave** en el sentido de que requiere atención
3. es **apreciable** en el sentido de que pueda ser objeto de estudio para su tratamiento
4. es **asumible** en el sentido de que no se van a tomar acciones para atajarlo

Las razones que pueden llevar a considerar un riesgo como **asumible** o **riesgo aceptable** son 4:

- cuando el impacto residual es asumible
- cuando el riesgo residual es asumible
- cuando el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgo residuales

Para este plan de seguridad se ha determinado el nivel de riesgo aceptable en el **nivel Medio (M).** Los activos que tengan una valoración de Riesgo total superior a esta puntuación (Riesgo Asumible) serán incluidos en el Plan de Gestión del Riesgos, donde se especificarán las acciones a tomar para disminuir el riesgo que soportan. Los controles a implantar, irán dirigidos a proteger de aquellas amenazas que cuenten con mayor Riesgo.

7. Salvaguardas, Impacto Residual y Riesgo Residual

En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto. En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tec-nológicos que reducen el riesgo. Hay amenazas que se pueden tratar simplemente organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), otras, seguridad física y, por último, está la política de personal.

Para los activos identificados en este plan se han considerado por motivos de simplicidad los tipos de salvaguardas relacionados en la tabla siguiente:

Abreviatura	Descrpción
PR	Preventivas
DR	Disuasorias
EL	Eliminatorias
IM	Minimizadoras
CR	Correctivas
RC	Recuperativas
MN	De Monitorización
DC	De Detección
AW	De Concienciación
AD	Administrativas

Tabla 20. Tipos de Salvaguardas

Las salvaguardas se han valorado de acuerdo a los niveles de capacidad de madurez utilizados para el análisis diferencial de este plan (Ver **tabla 3**). De forma que cuanto mayor es el nivel de madurez del proceso de implantación de una salvaguarda mayor efectividad se considera y mayor será en grado de disminución sobre la degradación original del activo. En los niveles más sencillos (L0 a L2) la efectividad de las salvaguardas es baja pero crece rápidamente, en los niveles superiores (L3 a L5) la efectividad es muy alta pero cada el paso al nivel superior sólo supone un pequeño incremente en la efectividad de la salvaguarda.

Valor	Efectividad	Significado	% Efectividad
L0	0	Proceso incompleto	0%
L1	0,1	Proceso Ejecutado	10%
L2	0,5	Proceso Gestionado	50%
L3	0,9	Proceso Establecido	90%
L4	0,95	Proceso Predecible	95%
L5	1	Proceso Optimizado	100%
L6	N/A	No aplica	N/A

Tabla 21. Efectividad de las Salvaguardas en función de su nivel de madurez

Las salvaguardas actúan sobre la degradación original del activo, disminuyéndola en el algún grado, pero también pueden actuar sobre la frecuencia de ocurrencia de la amenaza, disminuyéndola en un determinado grado igualmente. Para evaluar el nivel de efectividad de una salvaguarda sobre la frecuencia de la amenaza en el activo en función del nivel de madurez del proceso de implantación de la misma se ha utilizado la tabla siguiente:

	FRECUENCIA			
NIVEL CAPACIDAD	PF	FN	F	MF
L0	PF	FN	F	MF
L1	PF	FN	F	MF
L2	PF	PF	FN	F
L3	PF	PF	FN	F
L4	PF	PF	PF	FN
L5	PF	PF	PF	PF

Tabla 22. Efectividad de la Salvaguarda en función de su nivel de madurez

Por ejemplo, para una amenaza catalogada con una frecuencia **MF** (Muy Frecuente) sobre un activo sobre el que se ha incorporado una salvaguarda considerada en nivel de implantación **L1** la frecuencia no cambiaría y seguiría situada en el nivel **MF**, es decir, la salvaguarda no estaría actuando sobre la frecuencia de la amenaza. En cambio si incrementamos el nivel de madurez de la salvaguarda al nivel **L2** la frecuencia bajaría de **MF** a **F** con lo que podría reducirse el riesgo residual sobre el activo afectado por dicha amenaza.

Una vez determinado el nivel de riesgo aceptable como **MEDIO (M)** se analizarán las salvaguardas aplicadas a las amenazas evaluadas con un riesgo potencial superior, es decir, **ALTO (A)** y **MUY ALTO (MA).**

A partir de los activos con riesgo superior a **M** volvemos a calcular el impacto y el riesgo de igual forma que para el impacto potencial y el riesgo potencial, obteniendo de esta forma el **IMPACTO RESIDUAL Y EL RIESGO RESIDUAL**

El **Anexo X** relaciona los activos que pueden sufrir amenazas con un riesgo potencial **ALTO** o **MUY ALTO**, los tipos de salvaguardas que se les aplican junto con su nivel de implantación. Por último se calculan la **DEGRADACIÓN RESIDUAL, IMPACTO RESIDUAL y RIESGO RESIDUAL.**

Pueden consultarse todos los cálculos realizados en la hoja de cálculo adjunta denominada ***Analisis de Riegos V0.2.xlsx***

8. Resultados

Como resultado de la aplicación de las salvaguardas (Ver Anexo X) podemos observar como muchas de las amenazas se reducen a un nivel de riesgo aceptable o inferior de forma que nuevamente, teniendo en cuenta el nivel de riesgo aceptable, nos quedaremos con los activos cuyas amenazas superan este nivel. A continuación se muestra la tabla de activos con sus amenazas por encima del nivel de riesgo aceptable **(M)**.

Sigla	Descripción
V	Valor del Activo
I P	Impacto Potencial
R P	Riesgo Potencial
SV	Salvaguardas
DESCRIPCION	Descripción Salvaguardas
L	Nivel Madurez Salvaguardas
I R	Impacto Residual
R R	Riesgo Residual

ACTIVO	V	AMENAZA	I P	R P	SV	DESCRIPCION	L	I R	R R
cortafuegos	**A**								
		Ataque Destructivo	A	**MA**	DC	De Detección	L3	M	A
almacenamiento en red	**MA**								
		Errores del administrador	MA	**MA**	AW	De Concienciación	L2	MA	A
		Errores de Configuración	MA	**MA**	MN	De Monitorización	L2	MA	A
		Indisponibilidad del personal	MA	A	IM	Minimizadoras	L2	MA	A
servidor de presentación	**A**								
		Difusión de software dañino	M	**MA**	DC	De Detección	L3	M	A
servidor de aplicaciones	**A**								
		Difusión de software dañino	M	**MA**	DC	De Detección	L3	M	A
sistema de gestión de bases de datos	**A**								
		Difusión de software dañino	M	**MA**	DC	De Detección	L3	M	A
sistema operativo	**A**								
		Difusión de software dañino	M	**MA**	DC	De Detección	L3	M	A
		Caida del sistema por agotamiento de recursos	A	A	RC	Recuperativas	L0	A	A
gestor de máquinas virtuales	**A**								
		Difusión de software dañino	M	**MA**	DC	De Detección	L3	M	A
servidor de terminales	**A**								
		Difusión de software dañino	M	**MA**	DC	De Detección	L3	M	A
Datos de carácter personal nivel alto	**A**								

ACTIVO	V	AMENAZA	I P	R P	SV	DESCRIPCION	L	I R	R R
		Errores de los usuarios	A	MA	AW	De Concienciación	L2	A	MA
		Deficiencias en la organización	A	A	AD	Administrativas	L1	A	A
		Alteración de la información	A	MA	CR	Correctivas	L1	A	MA
		Introducción de información incorrecta	A	MA	CR	Correctivas	L1	A	MA
		Divulgación de la información	M	MA	AW	De Concienciación	L2	M	A
		Suplantación de la identidad del usuario	M	MA	AW	De Concienciación	L2	M	A
registro de actividad	**A**								
		Suplantación de la identidad del usuario	A	MA	AW	De Concienciación	L2	A	MA
Objetivos y Misión	**A**								
		Difusión de software dañino	M	MA	DC	De Detección	L3	M	A
		Escapes de información	A	MA	AW	De Concienciación	L2	A	MA
		Alteración de la información	A	MA	CR	Correctivas	L1	A	MA
		Introducción de información incorrecta	A	MA	CR	Correctivas	L1	A	MA
		Divulgación de la información	A	MA	AW	De Concienciación	L2	A	MA
		Indisponibilidad del personal	M	A	IM	Minimizadoras	L1	M	A
Imagen, reputación, credibilidad	**A**								
		Deficiencias en la organización	A	A	AD	Administrativas	L1	A	A
		Difusión de software dañino	M	MA	DC	De Detección	L3	M	A
		Escapes de información	A	MA	AW	De Concienciación	L2	A	MA
		Alteración de la información	A	MA	CR	Correctivas	L1	A	MA
		Introducción de información incorrecta	A	MA	CR	Correctivas	L1	A	MA
		Divulgación de la información	A	MA	AW	De Concienciación	L2	A	MA
		Indisponibilidad del personal	A	MA	IM	Minimizadoras	L1	A	MA
		Suplantación de la identidad del usuario	M	MA	AW	De Concienciación	L2	M	A
		Difusión de software dañino	M	MA	DC	De Detección	L3	M	A
Conocimiento acumulado	**A**								
		Indisponibilidad del personal	A	A	IM	Minimizadoras	L1	A	A
		Indisponibilidad del personal	A	A	IM	Minimizadoras	L1	A	A
Intimidad / Honor de las personas	**A**								
		Deficiencias en la organización	A	MA	AD	Administrativas	L1	A	MA
		Escapes de información	A	MA	AW	De Concienciación	L2	A	MA
		Suplantación de la identidad del usuario	A	MA	AW	De Concienciación	L2	A	MA
Integridad Fisica de las personas	**MA**								
		Errores de los usuarios	MA	MA	AW	De Concienciación	L2	MA	MA
		Errores del administrador	MA	MA	AW	De Concienciación	L2	MA	MA

ACTIVO	V	AMENAZA	I P	R P	SV	DESCRIPCION	L	I R	R R
		Errores de monitorización (log)	MA	**MA**	MN	De Monitorización	L2	MA	**MA**
		Errores de Configuración	MA	**MA**	DC	De Detección	L3	A	**MA**
		Deficiencias en la organización	MA	**MA**	AD	Administrativas	L1	MA	**MA**
		Introducción de información incorrecta	MA	**MA**	CR	Correctivas	L1	MA	**MA**
		Destrucción de la información	MA	**MA**	DC	De Detección	L3	A	A
		Indisponibilidad del personal	MA	**MA**	IM	Minimizadoras	L1	MA	**MA**
		Denegación de Servicio	MA	A	RC	Recuperativas	L1	MA	A

Tabla 23. Riesgo Residual para cada Amenaza

FASE 4: Propuestas de Proyectos.

1. Introducción

Una vez conocidos los riesgos a los que están sometidos los activos que forman parte del alcance de este plan podemos hacer propuestas que disminuyan el riesgo sobre dichos activos y por tanto mejoren el nivel de seguridad de la organización.

En resumen las amenazas que afectan a los activos con riesgo residual **ALTO** o **MUY ALTO** son las siguientes (por orden alfabético):

- Alteración de la información
- Ataque Destructivo
- Caida del sistema por agotamiento de recursos
- Deficiencias en la organización
- Denegación de Servicio
- Destrucción de la información
- Difusión de software dañino
- Divulgación de la información
- Errores de Configuración
- Errores de los usuarios
- Errores de monitorización (log)
- Errores del administrador
- Escapes de información
- Indisponibilidad del personal
- Introducción de información incorrecta
- Suplantación de la identidad del usuario

Estas amenazas pueden afectar de manera diferente a los diferentes activos, y para cada una de ellas se han considerado las salvaguardas implantadas (ver tabla 23), así como su nivel de implantación. En resumen, las salvaguardas consideradas han sido las siguientes (por orden alfabético)

- Administrativas
- Correctivas
- De Concienciación
- De Detección
- De Monitorización
- Minimizadoras
- Recuperativas

Teniendo en cuenta estas amenazas y las salvaguardas actuales propondremos a continuación en el "***Plan de Riesgos"***, los proyectos orientados a mitigar los riesgos detectados por encima del nivel asumible por la organización.

2. Plan de Riesgos

A continuación se presentan varias iniciativas estratégicas que a su vez se desglosarán en uno o más proyectos. Todas las iniciativas planteadas y los proyectos que se pueden desencadenar tienen como objetivo la mitigación de los riesgos detectados en el FASE 4 de este plan director. Para una descripción detallada de los proyectos incluidos en cada iniciativa ver el **Anexo XI** según se indica en el ***POE – SGSI – 0601 Análisis y Gestión de Riesgos***.

1.	**Plan de Formación**
	a. Concienciación a usuarios y profesionales TIC
	b. Formación a profesionales TIC (buenas prácticas, estándares, gestión de sistemas IDS/IPS)
	c. Formación a profesionales TIC sobre las metodologías para la gestión de incidentes
	d. Formación a profesionales TIC sobre las metodologías para la continuidad del negocio y la recuperación de desastres
	e. Formación a usuarios y profesionales TIC en Seguridad del Paciente
	f. Plan de difusión de sistemas de notificación de incidentes entre los usuarios
2.	**Proyecto para la mejora de la detección, notificación y gestión de incidentes**
	a. Planificación para la Prevención de incidentes
	b. Planificación para la Detección y Análisis de incidentes
	c. Planificación para la Contención de incidentes
	d. Planificación para la Resolución de incidentes
	e. Implantación de sistemas IDS/IPS
3.	**Plan para la continuidad del negocio y recuperación de desastres**
	a. Planificación de la Continuidad del Negocio y Recuperación de Desastres
	b. Implantación y Operación
	c. Seguimiento y Revisión
4.	**Plan de auditoría de los sistemas de información para la seguridad del paciente**
	a. Creación de los mecanismos organizativos para la evaluación de las tecnologías de la información y la seguridad del paciente.
	b. Plan de Auditoría de seguridad del paciente
	c. Auditoría de Seguridad del Paciente

Iniciativa de Proyecto: ***Plan de Formación***		**Descripción: Concienciación a usuarios y profesionales TIC sobre las amenazas más importantes y formación en buenas prácticas y metodologías para la reducción de los riesgos**	**Comité de iniciativa (propuesta):** **Responsable de Seguridad de la Información, Dirección de Recursos Humanos, Dirección TIC, Formación**
Proyectos de la iniciativa	**Alcance**	**Datos Principales**	**Beneficios**
PR-1A Concienciación a usuarios y profesionales TIC	Profesionales de Atención en Urgencias y profesionales TIC. Amenazas relacionadas con usuarios y profesionales TIC, los datos de carácter personal y la imagen y reputación de la organización	**Inicio:** lun 01/02/16 **Fin:** vie 26/02/16 **Relación con las iniciativas**: Proyecto para la mejora de la detección, notificación y gestión de incidentes.	**Estratégicos:** Se espera una reducción en los riesgos que afectan a la intimidad de los pacientes y la imagen y reputación de la organización. **Económicos:** No cuantificados. Es de esperar una mejora en los problemas relacionados con Divulgación de la información, Errores de los usuarios, Errores del administrador, Escapes de información y Suplantación de la identidad del usuario con el consiguiente ahorro económico en horas/hombre para la corrección de estos problemas.
PR-1B Formación a profesionales TIC (gestión de sistemas IDS/IPS)	Profesionales TIC. Gestión de sistemas IDS/IPX	**Inicio**: lun 29/02/16 **Fin**: vie 04/03/16 **Relación con las iniciativas:** Proyecto para la mejora de la detección, notificación y gestión de incidentes.	**Estratégicos:** Reducción de problemas relacionados con la difusión de software dañino que pueden afectar a la disponibilidad de los sistemas de información **Económicos:** No cuantificados. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la Difusión del Software Dañino.
PR-1C Formación a profesionales TIC sobre las metodologías para la gestión de incidentes	Profesionales TIC. Metodologías y buenas prácticas para la detección, notificación y gestión de incidentes	**Inicio:** lun 07/03/16 **Fin:** vie 11/03/16 **Relación con las iniciativas:** Proyecto para la mejora de la detección, notificación y gestión de incidentes.	**Estratégicos** Reducción de problemas relacionados con la difusión de software dañino que pueden afectar a la disponibilidad de los sistemas de información. **Económicos:** No cuantificados. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la disponibilidad de los sistemas
PR-1D Formación a profesionales TIC sobre las metodologías para la continuidad del	Profesionales TIC. Metodologías de continuidad del negocio y Recuperación de Destastres	**Inicio:** lun 14/03/16 **Fin:** vie 18/03/16 **Relación con las iniciativas:** *Plan para la Continuidad del Negocio y Recuperación de Desastres*	**Estratégicos:** Tiempos de respuesta más cortos en la recuperación de los sistemas de información en caso de falta de indisponibilidad. **Económicos:** No cuantificados. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la disponibilidad de los sistemas

Iniciativa de Proyecto: *Plan de Formación*		Descripción: Concienciación a usuarios y profesionales TIC sobre las amenazas más importantes y formación en buenas prácticas y metodologías para la reducción de los riesgos	Comité de iniciativa (propuesta): Responsable de Seguridad de la Información, Dirección de Recursos Humanos, Dirección TIC, Formación
negocio y la recuperación de desastres			
PR-1E Formación a usuarios y profesionales TIC en Seguridad del Paciente	Usuarios de Atención en Urgencias y Profesionales TIC. Seguridad del Paciente	**Inicio:** lun 21/03/16 **Fin:** vie 25/03/16 **Relación con las iniciativas:** *Plan de auditoría de los sistemas de información para la seguridad del paciente*	**Estratégicos:** Mejora en el diseño y uso de las Tecnologías de la Información Sanitarias en relación con la Seguridad del Paciente. Disminución de Eventos adversos en la salud del paciente **Económicos:** No cuantificados. Disminución en la estancia media de hospitalización, disminución de la repetición de pruebas diagnósticas innecesarias, disminución de intervenciones quirúrgicas innecesarias.
PR-1F Plan de difusión de sistemas de notificación de incidentes entre los usuarios	Usuarios de Atención en Urgencias	**Inicio:** lun 28/03/16 **Fin:** vie 01/04/16 ***Relación con las iniciativas:*** *Proyecto para la mejora de la detección, notificación y gestión de incidentes, Plan de auditoría de los sistemas de información para la seguridad del paciente.*	**Estratégicos**: Mejora en el diseño y uso de las Tecnologías de la Información Sanitarias en relación con la Seguridad del Paciente. Disminución de Eventos adversos en la salud del paciente. Reducción de problemas relacionados con la difusión de software dañino que pueden afectar a la disponibilidad de los sistemas de información **Económicos:** No cuantificados. Disminución en la estancia media de hospitalización, disminución de la repetición de pruebas diagnósticas innecesarias, disminución de intervenciones quirúrgicas innecesarias. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la disponibilidad de los sistemas

Iniciativa de Proyecto: ***Proyecto para la mejora de la detección, notificación y gestión de incidentes***		**Descripción: Planificación e implantación de los procedimientos para la detección, notificación y gestión de los incidentes**	**Comité de iniciativa (propuesta):** **Responsable de Seguridad de la Información, Dirección TIC**
Proyectos de la iniciativa	**Alcance**	**Datos Principales**	**Beneficios**
PR-2A Planificación para la Prevención de incidentes	Profesionales TIC. Plan para la prevención de incidentes para el Servicio de Atención en Urgencias	**Inicio:** lun 04/04/16 **Fin:** vie 08/04/16 **Relación con las iniciativas**: Plan para la continuidad del negocio y recuperación de desastres, Plan de Formación	**Estratégicos:** Reducción de problemas relacionados con la difusión de software dañino y otras amenazas que pueden afectar a la disponibilidad de los sistemas de información. **Económicos:** No cuantificados. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la Difusión del Software Dañino y otras amenazas que pueden afectar a la disponibilidad de los sistemas de información..
PR-2B Planificación para la Detección y Análisis de incidentes	Profesionales TIC. Plan para la Detección y Análisis de incidentes para el Servicio de Atención en Urgencias	**Inicio**: lun 11/04/16 **Fin**: vie 15/04/16 **Relación con las iniciativas:** Plan para la continuidad del negocio y recuperación de desastres, Plan de Formación	**Estratégicos:** Reducción de problemas relacionados con la difusión de software dañino y otras amenazas que pueden afectar a la disponibilidad de los sistemas de información. **Económicos:** No cuantificados. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la Difusión del Software Dañino y otras amenazas que pueden afectar a la disponibilidad de los sistemas de información..
PR-2C Planificación para la Contención de incidentes	Profesionales TIC. Plan para la Contención de incidentes para el Servicio de Atención en Urgencias	**Inicio:** lun 18/04/16 **Fin:** vie 22/04/16 **Relación con las iniciativas:** Plan para la continuidad del negocio y recuperación de desastres, Plan de Formación	**Estratégicos:** Reducción de problemas relacionados con la difusión de software dañino y otras amenazas que pueden afectar a la disponibilidad de los sistemas de información. **Económicos:** No cuantificados. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la Difusión del Software Dañino y otras amenazas que pueden afectar a la disponibilidad de los sistemas de información.
PR-2D Planificación para la Resolución de incidentes	Profesionales TIC. Plan de Resolución de Incidentes para el Servicio de Atención en Urgencias	**Inicio:** lun 25/04/16 **Fin:** vie 29/04/16 **Relación con las iniciativas:** Plan para la continuidad del negocio y recuperación de desastres, Plan de Formación	**Estratégicos:** Reducción de problemas relacionados con la difusión de software dañino y otras amenazas que pueden afectar a la disponibilidad de los sistemas de información. **Económicos:** No cuantificados. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de

Iniciativa de Proyecto: ***Proyecto para la mejora de la detección, notificación y gestión de incidentes***		**Descripción: Planificación e implantación de los procedimientos para la detección, notificación y gestión de los incidentes**	**Comité de iniciativa (propuesta):** **Responsable de Seguridad de la Información, Dirección TIC**
			incidentes relacionados con la Difusión del Software Dañino y otras amenazas que pueden afectar a la disponibilidad de los sistemas de información.
PR-2E Implantación de sistemas IDS/IPS	Profesionales TIC. Sistemas IDS/IPS para el Servicio de Atención en Urgencias	**Inicio:** lun 02/05/16 **Fin:** vie 06/05/16 **Relación con las iniciativas:** Plan para la continuidad del negocio y recuperación de desastres, Plan de Formación.	**Estratégicos:** Reducción de problemas relacionados con la difusión de software dañino y otras amenazas que pueden afectar a la disponibilidad de los sistemas de información. **Económicos:** No cuantificados. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la Difusión del Software Dañino y otras amenazas que pueden afectar a la disponibilidad de los sistemas de información.

Iniciativa de Proyecto: ***Plan para la continuidad del negocio y recuperación de desastres***		**Descripción: Planificación de los procedimientos para la continuidad del negocio y la recuperación de desastres**	**Comité de iniciativa (propuesta):** **Responsable de Seguridad de la Información, Dirección TIC, Dirección de Atención en Urgencias.**
Proyectos de la iniciativa	**Alcance**	**Datos Principales**	**Beneficios**
PR-3A Planificación de la Continuidad del Negocio y Recuperación de Desastres	Profesionales TIC. Plan para la Continuidad del Negocio y Recuperación de Desastres para el Servicio de Atención en Urgencias	**Inicio:** lun 09/05/16 **Fin:** vie 03/06/16 **Relación con las iniciativas**: Plan de Formación, Proyecto para la mejora de la detección, notificación y gestión de incidentes	**Estratégicos:** Reducción de problemas relacionados con amenazas que pueden afectar a la disponibilidad de los sistemas de información. **Económicos:** No cuantificados. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con amenazas que pueden afectar a la disponibilidad de los sistemas de información.
PR-3B Implantación y Operación	Profesionales TIC. Implantación del plan de continuidad del negocio para el Servicio de Atención en Urgencias	**Inicio**: lun 06/06/16 **Fin**: vie 10/06/16 **Relación con las iniciativas:** Plan de Formación, Proyecto para la mejora de la detección, notificación y gestión de incidentes	**Estratégicos:** Reducción de problemas relacionados con amenazas que pueden afectar a la disponibilidad de los sistemas de información. **Económicos:** No cuantificados. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con amenazas que pueden afectar a la disponibilidad de los sistemas de información.
PR-3C Seguimiento y Revisión	Profesionales TIC. Auditoría del plan de continuidad del negocio y recuperación de desastres.	**Inicio:** lun 13/06/16 **Fin:** vie 17/06/16 **Relación con las iniciativas:** Plan de Formación, Proyecto para la mejora de la detección, notificación y gestión de incidentes	**Estratégicos:** Mejora continua de los planes de continuidad del negocio y recuperación de desastres. **Económicos:** No cuantificados. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con amenazas que pueden afectar a la disponibilidad de los sistemas de información.

Iniciativa de Proyecto Plan de auditoría de los sistemas de información para la seguridad del paciente		**Descripción: Plan de auditoría para la mejora de las Tecnologías de la Información Sanitaria**	**Comité de iniciativa (propuesta):** Responsable de Seguridad de la Información, Dirección TIC, Dirección de Atención en Urgencias.
Proyectos de la iniciativa	**Alcance**	**Datos Principales**	**Beneficios**
PR-4A Creación de los mecanismos organizativos para la evaluación de las tecnologías de la información y la seguridad del paciente.	Profesionales TIC. Profesionales Atención en Urgenicas. Calidad. Seguridad del Paciente	**Inicio:** lun 20/06/16 **Fin:** vie 24/06/16 **Relación con las iniciativas**: Plan de Formación, Proyecto para la mejora de la detección, notificación y gestión de incidentes	**Estratégicos:** Mejora continua de los Sistemas de Información de Urgencias, Reducción de problemas relacionados con amenazas que pueden afectar a la disponibilidad de los sistemas de información. Reducción en los riesgos que afectan a la Misión, imagen y reputación de la organización. **Económicos:** No cuantificados. Disminución en la estancia media de hospitalización, disminución de la repetición de pruebas diagnósticas innecesarias, disminución de intervenciones quirúrgicas innecesarias. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la disponibilidad de los sistemas.
PR-4B Plan de Auditoría de seguridad del paciente	Profesionales TIC. Profesionales Atención en Urgenicas. Calidad. Seguridad del Paciente	**Inicio**: lun 27/06/16 **Fin**: vie 01/07/16 **Relación con las iniciativas:** Plan de Formación, Proyecto para la mejora de la detección, notificación y gestión de incidentes	**Estratégicos:** Reducción de Eventos Adversos en la Seguridad del Paciente. **Económicos:** No cuantificados. Disminución en la estancia media de hospitalización, disminución de la repetición de pruebas diagnósticas innecesarias, disminución de intervenciones quirúrgicas innecesarias. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la disponibilidad de los sistemas.
PR-4C Auditoría de Seguridad del Paciente	Profesionales TIC. Profesionales Atención en Urgenicas. Calidad. Seguridad del Paciente.	**Inicio:** lun 04/07/16 **Fin:** vie 29/07/16 **Relación con las iniciativas:** Plan de Formación, Proyecto para la mejora de la detección, notificación y gestión de incidentes	**Estratégicos:** Reducción de Eventos Adversos en la Seguridad del Paciente. **Económicos:** No cuantificados. Disminución en la estancia media de hospitalización, disminución de la repetición de pruebas diagnósticas innecesarias, disminución de intervenciones quirúrgicas innecesarias. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la disponibilidad de los sistemas.

El Anexo XI detalla cada una de las iniciativas propuestas junto con sus proyectos derivados según ***POE – SGSI – 0601 Análisis y Gestión de Riesgos***.

3. Planificación Temporal

Nombre de la Tarea	Duración	Comienzo	Fin
1.Plan de Formación	45 días	**lun 01/02/16**	**vie 01/04/16**
PR-1A Concienciación a usuarios y profesionales TIC	20 días	lun 01/02/16	vie 26/02/16
PR-1B Formación a profesionales TIC (buenas prácticas, estándares, gestión de sistemas IDS/IPS)	5 días	lun 29/02/16	vie 04/03/16
PR-1C Formación a profesionales TIC sobre las metodologías para la gestión de incidentes	5 días	lun 07/03/16	vie 11/03/16
PR-1D Formación a profesionales TIC sobre las metodologías para la continuidad del negocio y la recuperación de desastres	5 días	lun 14/03/16	vie 18/03/16
PR-1E Formación a usuarios y profesionales TIC en Seguridad del Paciente	5 días	lun 21/03/16	vie 25/03/16
PR-1F Plan de difusión de sistemas de notificación de incidentes entre los usuarios	5 días	lun 28/03/16	vie 01/04/16
2.Proyecto para la mejora de la detección, notificación y gestión de incidentes	25 días	**lun 04/04/16**	**vie 06/05/16**
PR-2A Planificación para la Prevención de incidentes	5 días	lun 04/04/16	vie 08/04/16
PR-2B Planificación para la Detección y Análisis de incidentes	5 días	lun 11/04/16	vie 15/04/16
PR-2C Planificación para la Contención de incidentes	5 días	lun 18/04/16	vie 22/04/16
PR-2D Planificación para la Resolución de incidentes	5 días	lun 25/04/16	vie 29/04/16
PR-2E Implantación de sistemas IDS/IPS	5 días	lun 02/05/16	vie 06/05/16
3.Plan para la continuidad del negocio y recuperación de desastres	30 días	**lun 09/05/16**	**vie 17/06/16**
PR-3A Planificación de la Continuidad del Negocio y Recuperación de Desastres	20 días	lun 09/05/16	vie 03/06/16
PR-3B Implantación y Operación	5 días	lun 06/06/16	vie 10/06/16
PR-3C Seguimiento y Revisión	5 días	lun 13/06/16	vie 17/06/16
4.Plan de auditoría de los sistemas de información para la seguridad del paciente	1 día	**lun 20/06/16**	**lun 20/06/16**
PR-4A Creación de los mecanismos organizativos para la evaluación de las tecnologías de la información y la seguridad del paciente.	5 días	lun 20/06/16	vie 24/06/16
PR-4B Plan de Auditoría de seguridad del paciente	5 días	lun 27/06/16	vie 01/07/16
PR-4C Auditoría de Seguridad del paciente	20 días	lun 04/07/16	vie 29/07/16

Tabla 24. Planificación Temporal para la Implantación de los Proyectos

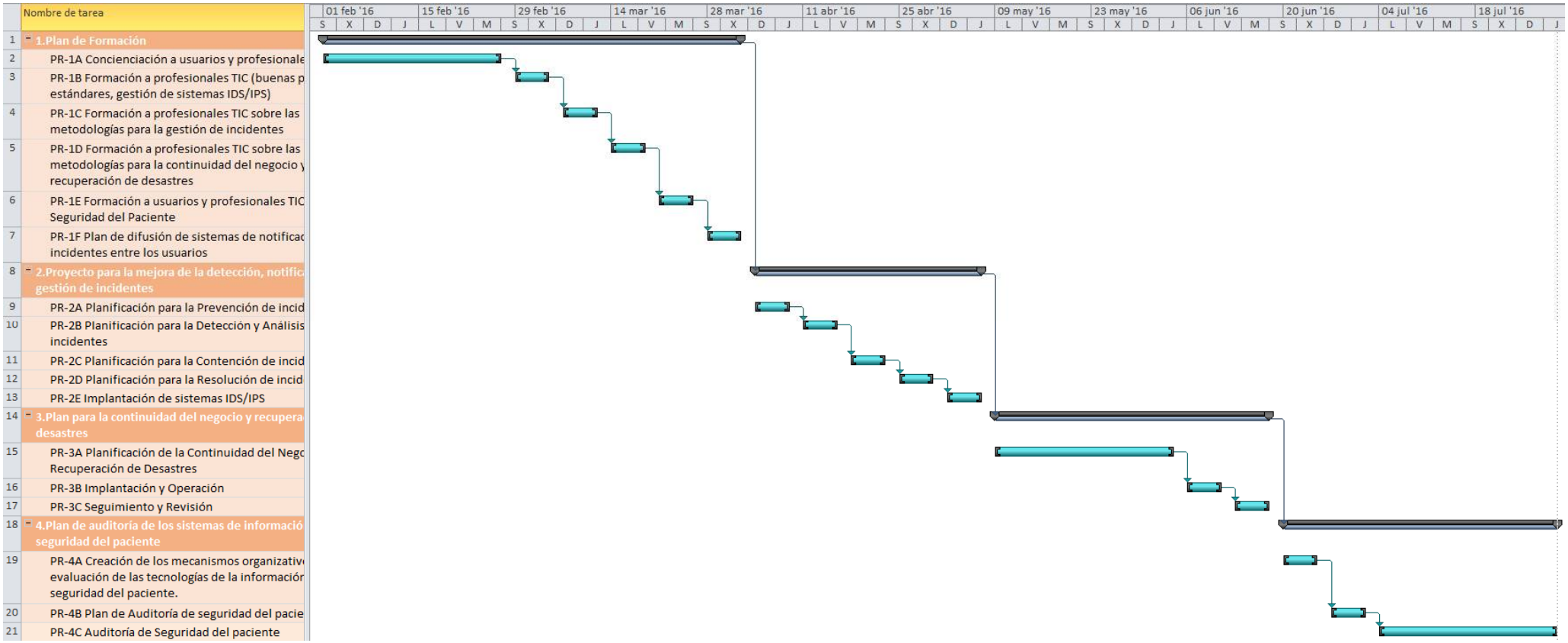


Ilustración 13. Planificación Temporal para la Implantación de los Proyectos

4. Propuesta Económica

Proyecto	Coste	Horas / hombre
1.Plan de Formación	27.630,00 €	
PR-1A Concienciación a usuarios y profesionales TIC	12.000,00 €	
PR-1B Formación a profesionales TIC (buenas prácticas, estándares, gestión de sistemas IDS/IPS)	4.500,00 €	
PR-1C Formación a profesionales TIC sobre las metodologías para la gestión de incidentes	3.500,00 €	
PR-1D Formación a profesionales TIC sobre las metodologías para la continuidad del negocio y la recuperación de desastres	3.500,00 €	
PR-1E Formación a usuarios y profesionales TIC en Seguridad del Paciente	3.500,00 €	
PR-1F Plan de difusión de sistemas de notificación de incidentes entre los usuarios	630,00 €	35
2.Proyecto para la mejora de la detección, notificación y gestión de incidentes	17.040,00 €	
PR-2A Planificación para la Prevención de incidentes	1.260,00 €	70
PR-2B Planificación para la Detección y Análisis de incidentes	1.260,00 €	70
PR-2C Planificación para la Contención de incidentes	1.260,00 €	70
PR-2D Planificación para la Resolución de incidentes	1.260,00 €	70
PR-2E Implantación de sistemas IDS/IPS	12.000,00 €	
3.Plan para la continuidad del negocio y recuperación de desastres	14.520,00 €	
PR-3A Planificación de la Continuidad del Negocio y Recuperación de Desastres	12.000,00 €	280
PR-3B Implantación y Operación	1.260,00 €	70
PR-3C Seguimiento y Revisión	1.260,00 €	70
4.Plan de auditoría de los sistemas de información para la seguridad del paciente	15.120,00 €	
PR-4A Creación de los mecanismos organizativos para la evaluación de las tecnologías de la información y la seguridad del paciente.	1.260,00 €	70
PR-4B Plan de Auditoría de seguridad del paciente	1.260,00 €	70
PR-4C Auditoría de Seguridad del paciente	12.600,00 €	700
total	**74.310,00 €**	**1.575**

Tabla 25. Propuesta Económica Para la Implantación de los Proyectos

5. Evolución del Riesgo Tras la Implantación de los Proyectos

La figura siguiente muestra como todos los riesgos que resultaron por encima del nivel **M** (Riesgo tolerable) en el análisis de riesgos anterior son tratados por uno o varios de los proyectos propuestos.

	Proyectos																	
Amenaza	PR-1A	PR-1B	PR-1C	PR-1D	PR-1E	PR-1F	PR-2A	PR-2B	PR-2C	PR-2D	PR-2E	PR-3A	PR-3B	PR-3C	PR-4A	PR-4B	PR-4C	**Tratamiento**
Alteración de la información					■										■	■	■	4
Ataque Destructivo				■			■	■	■	■	■	■	■	■				9
Caida del sistema por agotamiento de recursos				■								■	■	■				4
Deficiencias en la organización				■		■									■	■	■	5
Denegación de Servicio				■		■	■	■	■	■	■							7
Destrucción de la información					■		■	■	■	■	■	■	■	■				10
Difusión de software dañino		■	■				■	■	■	■	■	■	■	■				10
Divulgación de la información	■							■	■									4
Errores de Configuración						■	■	■	■	■	■				■	■	■	9
Errores de monitorización (log)						■	■	■	■	■	■				■	■	■	9
Errores del administrador	■					■									■	■	■	5
Errores de los usuarios	■				■	■									■	■	■	6
Escapes de información	■					■									■	■	■	5
Indisponibilidad del personal				■	■													3
Introducción de información incorrecta															■	■	■	3
Suplantación de la identidad del usuario	■							■	■	■								4

Tabla 26. Tratamiento de los Riesgos por los proyectos propuestos

De la misma forma cada proyecto aporta una serie de salvaguardas a los sistemas. La tabla siguiente muestra las salvaguardas que cada proyecto aporta.

	Salvaguardas						
Proyectos	AD Administrativas	AW De Concienciación	CR Correctivas	DC De Detección	IM Minimizadoras	MN De Monitorización	RC Recuperativas
PR-1A		■					
PR-1B		■					
PR-1C		■					
PR-1D		■					
PR-1E		■					
PR-1F		■					
PR-2A				■			
PR-2B						■	
PR-2C					■		
PR-2D			■			■	
PR-2E			■	■	■	■	
PR-3A							■
PR-3B							■
PR-3C	■					■	■
PR-4A	■	■					
PR-4B	■	■					
PR-4C	■	■	■	■	■	■	

Tabla 27. Salvaguardas aportadas por cada proyecto

Por otro lado, atendiendo a las nuevas salvaguardas previstas por los proyectos propuestos se considera que el nivel de capacidad de madurez de las mismas cambiará según la tabla siguiente, afectando al impacto residual actual y a la frecuencia de las amenazas, dando lugar a un nuevo riesgo potencial.

Amenazas		Salvaguardas	Nivel Actual	Nivel Nuevo
Alteración de la información	CR	Correctivas	L1	L2
Ataque Destructivo	DC	De Detección	L3	L4
Caida del sistema por agotamiento de recursos	RC	Recuperativas	L0	L2
Deficiencias en la organización	AD	Administrativas	L1	L2
Denegación de Servicio	RC	Recuperativas	L1	L2
Destrucción de la información	DC	De Detección	L3	L4
Difusión de software dañino	DC	De Detección	L3	L4
Divulgación de la información	AW	De Concienciación	L2	L3
Errores de Configuración	MN	De Monitorización	L2	L3
Errores de los usuarios	AW	De Concienciación	L2	L3
Errores de monitorización (log)	MN	De Monitorización	L2	L3

Amenazas		Salvaguardas	Nivel Actual	Nivel Nuevo
Errores del administrador	AW	De Concienciación	L2	L3
Escapes de información	AW	De Concienciación	L2	L3
Indisponibilidad del personal	IM	Minimizadoras	L2	L3
Introducción de información incorrecta	CR	Correctivas	L1	L2
Suplantación de la identidad del usuario	AW	De Concienciación	L2	L3

Tabla 28. Nuevos niveles de capacidad de madurez de las salvaguardas

Aplicando los nuevos niveles de madurez de las salvaguardas obtendremos un nuevo riesgo residual:

ACTIVO	V	AMENAZA	I P	R P	SV	DESCRIPCION	L	I R	R R
cortafuegos	**A**								
		Ataque Destructivo	A	**MA**	DC	De Detección	L4	M	M
almacenamiento en red	**MA**								
		Errores del administrador	MA	**MA**	AW	De Concienciación	L3	A	M
		Errores de Configuración	MA	**MA**	MN	De Monitorización	L3	A	M
		Indisponibilidad del personal	MA	A	IM	Minimizadoras	L3	A	M
servidor de presentación	**A**								
		Difusión de software dañino	M	**MA**	DC	De Detección	L4	M	M
servidor de aplicaciones	**A**								
		Difusión de software dañino	M	**MA**	DC	De Detección	L4	M	M
sistema de gestión de bases de datos	**A**								
		Difusión de software dañino	M	**MA**	DC	De Detección	L4	M	M
sistema operativo	**A**								
		Difusión de software dañino	M	**MA**	DC	De Detección	L4	M	M
		Caida del sistema por agotamiento de recursos	A	A	RC	Recuperativas	L4	A	M
gestor de máquinas virtuales	**A**								
		Difusión de software dañino	M	**MA**	DC	De Detección	L4	M	M
servidor de terminales	**A**								
		Difusión de software dañino	M	**MA**	DC	De Detección	L4	M	M
Datos de carácter personal nivel alto	**A**								
		Errores de los usuarios	A	**MA**	AW	De Concienciación	L3	M	**A**
		Deficiencias en la organización	A	A	AD	Administrativas	L2	M	B

ACTIVO	V	AMENAZA	I P	R P	SV	DESCRIPCION	L	I R	R R
		Alteración de la información	A	MA	CR	Correctivas	L2	A	MA
		Introducción de información incorrecta	A	MA	CR	Correctivas	L2	A	MA
		Divulgación de la información	M	MA	AW	De Concienciación	L3	M	A
		Suplantación de la identidad del usuario	M	MA	AW	De Concienciación	L3	M	A
registro de actividad	**A**								
		Suplantación de la identidad del usuario	A	MA	AW	De Concienciación	L3	A	A
Objetivos y Misión	**A**								
		Difusión de software dañino	M	MA	DC	De Detección	L4	M	M
		Escapes de información	A	MA	AW	De Concienciación	L3	M	A
		Alteración de la información	A	MA	CR	Correctivas	L2	A	MA
		Introducción de información incorrecta	A	MA	CR	Correctivas	L2	A	MA
		Divulgación de la información	A	MA	AW	De Concienciación	L3	M	A
		Indisponibilidad del personal	M	A	IM	Minimizadoras	L3	M	M
Imagen, reputación, credibilidad	**A**								
		Deficiencias en la organización	A	A	AD	Administrativas	L2	A	M
		Difusión de software dañino	M	MA	DC	De Detección	L4	M	M
		Escapes de información	A	MA	AW	De Concienciación	L3	M	A
		Alteración de la información	A	MA	CR	Correctivas	L2	A	MA
		Introducción de información incorrecta	A	MA	CR	Correctivas	L2	A	MA
		Divulgación de la información	A	MA	AW	De Concienciación	L3	M	A
		Indisponibilidad del personal	A	MA	IM	Minimizadoras	L3	M	M
		Suplantación de la identidad del usuario	M	MA	AW	De Concienciación	L3	M	A
		Difusión de software dañino	M	MA	DC	De Detección	L4	M	M
Conocimiento acumulado	**A**								
		Indisponibilidad del personal	A	A	IM	Minimizadoras	L3	M	B
		Indisponibilidad del personal	A	A	IM	Minimizadoras	L3	M	B
Intimidad / Honor de las personas	**A**								
		Deficiencias en la organización	A	MA	AD	Administrativas	L3	A	A
		Escapes de información	A	MA	AW	De Concienciación	L3	M	A
		Suplantación de la identidad del usuario	A	MA	AW	De Concienciación	L3	M	A

ACTIVO	V	AMENAZA	I P	R P	SV	DESCRIPCION	L	I R	R R
Integridad Fisica de las personas	**MA**								
		Errores de los usuarios	MA	**MA**	AW	De Concienciación	L3	A	**MA**
		Errores del administrador	MA	**MA**	AW	De Concienciación	L3	A	**MA**
		Errores de monitorización (log)	MA	**MA**	MN	De Monitorización	L3	A	**MA**
		Errores de Configuración	MA	**MA**	DC	De Detección	L4	M	**M**
		Deficiencias en la organización	MA	**MA**	AD	Administrativas	L2	MA	**MA**
		Introducción de información incorrecta	MA	**MA**	CR	Correctivas	L2	MA	**MA**
		Destrucción de la información	MA	**MA**	DC	De Detección	L4	M	B
		Indisponibilidad del personal	MA	**MA**	IM	Minimizadoras	L3	A	**M**
		Denegación de Servicio	MA	A	RC	Recuperativas	L2	MA	A

Como se puede observar el nuevo riesgo residual baja hasta el nivel aceptable **(M)** o incluso por debajo **(B)**, sin embargo, algunos de los riesgos permanecen por encima del umbral aceptable. Por ello, y según se indica en el apartado ***5.8.1.3. Controles Ineficaces*** del ***POE – SGSI – 0601 Análisis y Gestión de Riesgos***, añadiremos nuevas salvaguardas a estos riesgos que permanecen por encima del umbral aceptable en función de las salvaguardas que añaden los proyectos propuestos para cada amenaza, recalculando el riesgo potencial hasta dejarlo en el nivel aceptable o por debajo del mismo. Este proceso sólo lo realizarmos para aquellas amenazas que superan el riesgo aceptable (**M**).

Por ejemplo, para el activo **Datos de Carácter personal nivel alto**, la amanaza **Errores de los usuarios** permenece con un riesgo Alto (**A**) después de subir el nivel de capacidad de madurez de la salvaguarda **De Concienciación** (**AW**) desde el nivel L2 a L3 como consencuencia de la implantación de los proyectos propuestos. Por tanto, añadimos una nueva salvaguarda, en este caso **De Monitorización (MN)**, que se encuentra en nivel **L2.** Volvemos a calcular la **REDUCCIÓN DE LA DEGRADACIÓN**, pero lo hacemos sobre la **DEGRADACIÓN RESIDUAL ANTERIOR**, (fruto de aplicar la salvaguarda AW), en lugar de sobre la **DEGRADACIÓN INICIAL**. De esta forma, calculamos la nueva **DEGRADACIÓN RESIDUAL** (1), la **REDUCCIÓN DE LA FRECUENCIA** (PF), el **IMPACTO RESIDUAL** (M) y por último, el nuevo **RIESGO RESIDUAL** (B). Como se puede observar en la tabla siguiente, todos los riesgos ALTO y MUY ALTO, bajan a riesgo BAJO, después de aplicar las nuevas salvaguardas.

Para escoger las nuevas salvaguardas aplicadas buscamos en la tabla nº 24 la amenaza "Errores de los usuarios" que será tratada por los proyectos PR-1A, PR-1E, PR-4A, PR-4B, PR-4C. En la tabla 25, se muestran las salvaguardas provistas por estos proyectos. Seleccionamos la que nos parezca más adecuada, distinta de la salvaguarda actual, y le asiganamos su nivel de madurez (tabla 26). Para este ejemplo podemos ver que las salvaguardas provistas son: De Concienciación, Administrativas, Correctivas, De Detección, Minimizadoras y De Monitorización.

En la hoja *"**Mejora 2**"* del archivo *"**Análisis de Riegos V0.2.xlsx**"* se pueden observar los cálculos realizados para obtener el nuevo nivel de riesgo de acuerdo con el ***POE – SGSI – 0601 Análisis y Gestión de Riesgos***. En las páginas siguientes se muestra el resultado final del riesgo para los activos seleccionados.

D	PERA	Datos de carácter personal nivel alto	A

AMENAZA	FRECUENCIA	DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDAS	DESCRIPCION	NIVEL IMPLANTACIÓN	Efectividad	REDUCCION DEGRADACIÓN	DEGRADACIÓN RESIDUAL	REDUCCIÓN FRECUENCIA	IMPACTO RESIDUAL	RIESGO RESIDUAL PARCIAL	RIESGO RESIDUAL
Errores de los usuarios	4	100	A	MA	AW	De Concienciación	L3	0,9	10	10	F	M	A	
					MN	De Monitorización	L2	0,5	5	1	PF	M	B	B
Alteración de la información	4	100	A	MA	CR	Correctivas	L2	0,5	50	50	F	A	MA	
					AW	De Concienciación	L3	0,9	5	1	PF	M	B	B
Introducción de información incorrecta	4	100	A	MA	CR	Correctivas	L2	0,5	50	50	F	A	MA	
					DC	De Detección	L3	0,9	5	1	PF	M	B	B
Divulgación de la información	4	10	M	MA	AW	De Concienciación	L3	0,9	1	1	F	M	A	
					MN	De Monitorización	L3	0,9	0,1	1	PF	M	B	B
Suplantación de la identidad del usuario	4	1	M	MA	AW	De Concienciación	L3	0,9	0,1	1	F	M	A	
					IM	Minimizadoras	L3	0,9	0,1	1	PF	M	B	B

D			**LOG**			**registro de actividad**						**A**			
AMENAZA	**FRECUENCIA**	**DEGRADACIÓN**	**IMPACTO POTENCIAL**	**RIESGO POTENCIAL**	**SALVAGUARDAS**	**DESCRIPCION**	**NIVEL IMPLANTACIÓN**	**Efectividad**	**REDUCCION DEGRADACIÓN**	**DEGRADACIÓN RESIDUAL**	**REDUCCIÓN FRECUENCIA**	**IMPACTO RESIDUAL**	**RIESGO RESIDUAL PARCIAL**	**RIESGO RESIDUAL**
Suplantación de la identidad del usuario	MF	100	A	**MA**	AW	De Concienciación	L3	0,9	10	10	F	M	A	
					IM	Minimizadoras	L3	0,9	1	1	PF	M	B	**B**

	O		O	Objetivos y Misión							A			
AMENAZA	FRECUENCIA	DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDAS	DESCRIPCION	NIVEL IMPLANTACIÓN	Efectividad	REDUCCION DEGRADACIÓN	DEGRADACIÓN RESIDUAL	REDUCCIÓN FRECUENCIA	IMPACTO RESIDUAL	RIESGO RESIDUAL PARCIAL	RIESGO RESIDUAL
Escapes de información	MF	100	A	MA	AW	De Concienciación	L3	0,9	10	10	F	M	A	
					MN	De Monitorización	L3	0,9	1	1	PF	M	B	B
Alteración de la información	MF	100	A	MA	CR	Correctivas	L2	0,5	50	50	F	A	MA	
					MN	De Monitorización	L3	0,9	5	1	PF	M	B	B
Introducción de información incorrecta	MF	100	A	MA	CR	Correctivas	L2	0,5	50	50	F	A	MA	
					DC	De Detección	L3	0,9	5	1	PF	M	B	B
Divulgación de la información	MF	100	A	MA	AW	De Concienciación	L3	0,9	10	10	F	M	A	
					MN	De Monitorización	L3	0,9	1	1	PF	M	B	B

IMG	IMG	Imagen, reputación, credibilidad	A

AMENAZA	FRECUENCIA	DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDAS	DESCRIPCION	NIVEL IMPLANTACIÓN	Efectividad	REDUCCION DEGRADACIÓN	DEGRADACIÓN RESIDUAL	REDUCCIÓN FRECUENCIA	IMPACTO RESIDUAL	RIESGO RESIDUAL PARCIAL	RIESGO RESIDUAL
Escapes de información	MF	100	A	MA	AW	De Concienciación	L3	0,9	10	10	F	M	A	
					MN	De Monitorización	L3	0,9	1	1	PF	M	B	B
Alteración de la información	MF	100	A	MA	CR	Correctivas	L2	0,5	50	50	F	A	MA	
					MN	De Monitorización	L3	0,9	5	1	PF	M	B	B
Introducción de información incorrecta	MF	100	A	MA	CR	Correctivas	L2	0,5	50	50	F	A	MA	
					DC	De Detección	L3	0,9	5	1	PF	M	B	B
Divulgación de la información	MF	100	A	MA	AW	De Concienciación	L3	0,9	10	10	F	M	A	
					MN	De Monitorización	L3	0,9	1	1	PF	M	B	B
Suplantación de la identidad del usuario	MF	10	M	MA	AW	De Concienciación	L3	0,9	1	1	F	M	A	
					IM	Minimizadoras	L3	0,9	0,1	1	PF	M	B	B

IP	IP	Intimidad / Honor de las personas	A

AMENAZA	FRECUENCIA	DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDAS	DESCRIPCION	NIVEL IMPLANTACIÓN	Efectividad	REDUCCION DEGRADACIÓN	DEGRADACIÓN RESIDUAL	REDUCCIÓN FRECUENCIA	IMPACTO RESIDUAL	RIESGO RESIDUAL PARCIAL	RIESGO RESIDUAL
Deficiencias en la organización	F	100	A	MA	AD	Administrativas	L2	0,5	50	50	FN	A	A	
					AW	De Concienciación	L3	0,9	5	1	PF	M	B	B
Escapes de información	MF	100	A	MA	AW	De Concienciación	L3	0,9	10	10	F	M	A	
					MN	De Monitorización	L3	0,9	1	1	PF	M	B	B
Suplantación de la identidad del usuario	MF	100	A	MA	AW	De Concienciación	L3	0,9	10	10	F	M	A	
					IM	Minimizadoras	L3	0,9	1	1	PF	M	B	B

IF	IF	Integridad Fisica de las personas	MA

AMENAZA	FRECUENCIA	DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDAS	DESCRIPCION	NIVEL IMPLANTACIÓN	Efectividad	REDUCCION DEGRADACIÓN	DEGRADACIÓN RESIDUAL	REDUCCIÓN FRECUENCIA	IMPACTO RESIDUAL	RIESGO RESIDUAL PARCIAL	RIESGO RESIDUAL
Errores de los usuarios	MF	100	MA	MA	AW	De Concienciación	L3	0,9	10	10	F	A	MA	
					MN	De Monitorización	L3	0,9	1	1	PF	M	B	B
Errores del administrador	MF	100	MA	MA	AW	De Concienciación	L3	0,9	10	10	F	A	MA	
					MN	De Monitorización	L3	0,9	1	1	PF	M	B	B
Errores de monitorización (log)	MF	100	MA	MA	MN	De Monitorización	L3	0,9	10	10	F	A	MA	
					IM	Minimizadoras	L3	0,9	1	1	PF	M	B	B
Deficiencias en la organización	MF	100	MA	MA	AD	Administrativas	L2	0,5	50	50	F	MA	MA	
					AW	De Concienciación	L3	0,9	5	1	PF	M	B	B
Introducción de información incorrecta	MF	100	MA	MA	CR	Correctivas	L2	0,5	50	50	F	MA	MA	
					AW	De Concienciación	L3	0,9	5	1	PF	M	B	B
Denegación de Servicio	PF	100	MA	A	RC	Recuperativas	L2	0,5	50	50	PF	MA	A	
					DC	De Detección	L3	0,9	5	1	PF	M	B	B

6. Evolución del Cumplimiento Tras la Implantación de los Proyectos Propuestos

El desarrollo e implantación de los proyectos propuestos debería suponer ciertas mejoras sobre el SGSI, afectando con una mejora en varios de los dominios de la norma ISO/IEC 27002:2013. La tabla siguiente relaciona cada uno de los dominios de la norma junto con los controles y cada uno de los proyectos que le afectaría.

DOMINIO ISO 27002:2013	CONTROLES AFECTADOS	PROYECTO ASOCIADO
A.5 Políticas de la Seguridad de la Información	A.5.1.1, A.5.1.2	PR-2A, PR-3A, PR-4A
A.6 Organización de la seguridad de la Información	A.6.1.2, A.6.1.1, A.6.1.4, A.6.1.5	PR-2A, PR-3A, PR-4A, PR-4B
A.7 Seguridad de RRHH	A.7.2.1, A.7.2.2	PR-1A,
A.8 Gestión de activos		
A.9 Control acceso		
A.10 Criptografía		
A.11 Seguridad física y ambiental		
A.12 Operaciones de seguridad	A.12.2.1, A.12.3.1 A.12.4.1, A.12.4.2, A.12.4.3, A.12.7.1, A.12.1.4,	PR-1E , PR-2E, PR-3B, PR-4B
A.13 Seguridad de las comunicaciones		
A.14 Adquisición, desarrollo y mantenimiento de sistemas	A.14.1.1, A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9, A.14.3.1	PR-4B
A.15 Relaciones con proveedores		
A.16 Gestión de Incidentes de Seguridad de la información	A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7	PR-1B, PR-1C, PR-1E,PR-1F, PR-2A, PR-2B, PR-2C, PR-2D, PR-2E
A.17 Aspectos de la seguridad de la información de la gestión de la continuidad del negocio	A.17.1.1, A.17.1.2, A.17.1.3, A.17.2.1	PR-1D, PR-2D, PR-3A, PR-3B, PR-3C
A.18 Cumplimiento	A.18.1, A.18.2	PR-1A, PR-4B

Tabla 29. Dominios y Controles afectados por los proyectos propuestos

La implantación de los proyectos propuestos provocaría una mejora en los niveles de madurez de los controles afectados en distinto grado. El archivo ***Anexo_XII_Analisis Diferencial_ISO_27002_2013.xlsx*** contiene los cambios sufridos en cada control respecto del análisis diferencial inicial (ver archivo ***Anexo_2_Analisis Diferencial_ISO_27002_2013.xlsx***)

Conviene destacar el importante impacto del proyecto **PR-4B**, que consiste en la implantación de un plan de auditoría mediante la utilización de la metodología de evaluación de las tecnologías de la información sanitarias proporcionada las guías SAFER[1]. Esta metodología

[1] https://www.healthit.gov/safer/safer-guides

aborda los eventos adversos de la seguridad del paciente ocasionados por las TIS[2] desde 8 dimensiones diferentes pero complementarias. De hay su alto impacto en algunos de los dominios de la ISO/IEC 27002:2013, especialmente en A.6. Organización de la seguridad de la Información, A.12 Operaciones de seguridad, A.14 Adquisición, desarrollo y mantenimiento de sistemas y A.18 Cumplimiento.

Las 9 Guías abordan los siguientes aspectos en profundidad, provocando mejoras en el desarrollo seguro, uso seguro y monitorización de la seguridad de las TIS. La tabla siguiente muestra los procesos abordados por las Guías SAFER.

Nombre de la Guía	Descripción de cada guía
Prácticas de alta prioridad	El subconjunto de procesos que determina qué es de "alto riesgo" y "alta prioridad", destinado a cubrir ampliamente todas las áreas que tienen un papel en la seguridad de los EHR.
Entrada automatizada de peticiones de asistencia con apoyo a la decisión	Los procesos relativos a la petición electrónica de medicamentos y pruebas de diagnóstico y ayudar al proceso de toma de decisiones clínicas en el punto de atención.
Informes de resultados de pruebas y su seguimiento	Procesos implicados en la entrega de resultados de las pruebas a los profesionales apropiados.
comunicación clínica	Los procesos de comunicación en 3 zonas de alto riesgo: consultas o derivaciones, comunicaciones de altas, y los mensajes relacionados con el paciente entre los médicos.
identificación de pacientes	Los procesos relacionados con la creación de nuevos pacientes en el EHR, registro de pacientes, recuperación de información sobre pacientes previamente registrados, y otros procesos de identificación de pacientes.
Planes de contingencia	Los procesos y los preparativos que deben estar en vigor en caso de que el EHR experimente un fallo hardware, software, o fallo de alimentación.
configuración del sistema	Los procesos necesarios para crear y mantener el entorno físico en el que funcionará el EHR, así como las infraestructuras relacionadas con el hardware y el software necesarios para ejecutar el EHR.
interfaces de sistema	Los procesos que permiten a diferentes dispositivos de hardware y aplicaciones de software conectarse tanto física como lógicamente para que puedan comunicarse y compartir información.
responsabilidades de organización	Las actividades organizativas, procesos y tareas que deben llevar a cabo las personas para garantizar la implantación del EHR seguro y eficaz y la operación continua.

Tabla 30. Guías SAFER y los procesos abordados

La tabla y la figura siguientes muestran la evolución del cumplimiento de la norma ISO/IEC 27002:2013.

[2] Tecnologías de la Información Sanitaria

	Dominio	% Conf Despues	% Conf Antes
A.5	POLÍTICAS DE SEGURIDAD	90%	10%
A.6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.	47%	29%
A.7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	61%	42%
A.8	GESTIÓN DE ACTIVOS.	15%	15%
A.9	CONTROL DE ACCESOS.	8%	8%
A.10	CIFRADO.	10%	10%
A.11	SEGURIDAD FÍSICA Y AMBIENTAL.	31%	31%
A.12	SEGURIDAD EN LA OPERATIVA.	53%	8%
A.13	SEGURIDAD EN LAS TELECOMUNICACIONES.	23%	23%
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	70%	12%
A.15	RELACIONES CON SUMINISTRADORES.	4%	4%
A.16	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	90%	1%
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	90%	5%
A.18	CUMPLIMIENTO.	81%	25%

Tabla 31. Evolución del cumplimiento ISO/IEC 27002:2013 por Dominios

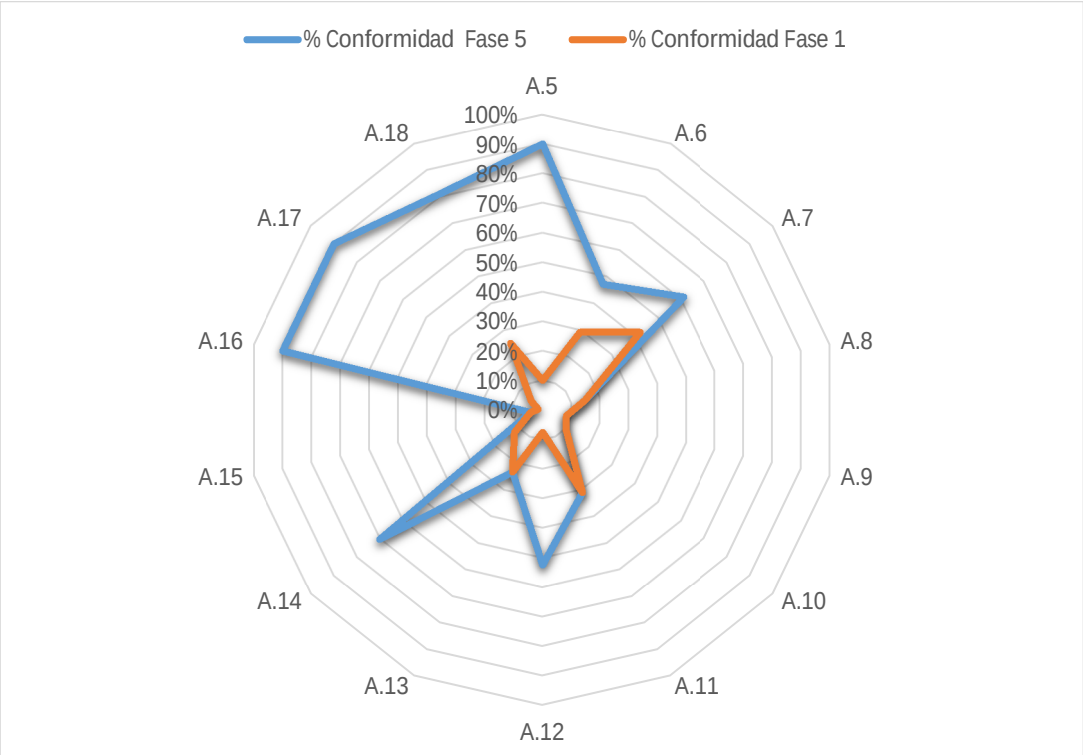


Ilustración 14. Evolución del cumplimiento ISO/IEC 27002:2013 por Dominios

FASE 5: Auditoría de Cumplimiento.

1. Introducción

El objetivo de la fase 5, Auditoría de Cumplimiento, es comprobar el nivel de madurez de la seguridad de la información para el alcance planteado para este proyecto (Servicio de Atención en Urgencias), después de la puesta en marcha de este plan director de seguridad de la información. Para ello tomaremos como referencia los 14 dominios, 35 objetivos y 114 controles de la norma 27002:2013.

2. Metodología

Apoyándonos en los controles propuestos por la norma ISO/IEC 27002 evaluaremos la madurez de cada uno de los 114 controles según el modelo de evaluación de procesos de la norma ISO/IEC 15504 mostrado en la tabla siguiente:

Valor	Efectividad	Significado	Descripción
L0	0%	Proceso incompleto	El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.
L1	10%	Proceso Ejecutado	El proceso implementado alcanza su propósito
L2	50%	Proceso Gestionado	El proceso ejecutado descrito anteriormente está ya implementado de forma gestionada (planificado, supervisado y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.
L3	90%	Proceso Establecido	El proceso gestionado descrito anteriormente está ahora implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso. La implantación de los procesos se ha estandarizado (se documenta, se comunica y se da formación)
L4	95%	Proceso Predecible	El proceso establecido descrito anteriormente ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.
L5	100%	Proceso Optimizado	El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con las metas presentes y futuras.
L6	N/A	No aplica	

Tabla 32. Modelo de evaluación de procesos ISO/IEC 15504

Evaluaremos por tanto el cumplimiento de los diferentes controles para cada dominio y el cumplimiento de los objetivos de control se obtendrá a partir del promedio de los controles de dicho objetivo de control. Por último, el nivel de cumplimiento o efectividad de las salvaguardas de cada dominio se obtendrá a partir del promedio de cumplimiento de sus objetivos de control.

Dominio n	% cumplimiento del Dominio (promedio de Objetivos de Control del Dominio)
Objetivo de Control 1	% cumplimiento Objetivo de Control 1 (Promedio de controles del objetivo de control)
Control 1	% cumplimiento control 1
Control 2	% cumplimiento control 2
Control 3	% cumplimiento control 3
Objetivo de Control 2	% cumplimiento Objetivo de Control 2 (Promedio de controles del objetivo de control)
Control 4	% cumplimiento control 4
Control 5	% cumplimiento control 5
Control 6	% cumplimiento control 6

Tabla 33. Ejemplo de Cálculo del 5 de cumplimiento por Dominio

3. Evaluación de Madurez

En el ANEXO XII se muestra la evolución del cumplimiento de los controles de la Norma ISO/IEC 27002 para cada uno de los Dominios de la misma. La tabla siguiente muestra el resumen de la evolución agrupado por dominios.

Dominio		% Conformidad Fase 1	% Conformidad Fase 5
A.5	POLÍTICAS DE SEGURIDAD	10%	90%
A.6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.	29%	47%
A.7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	42%	61%
A.8	GESTIÓN DE ACTIVOS.	15%	15%
A.9	CONTROL DE ACCESOS.	8%	8%
A.10	CIFRADO.	10%	10%
A.11	SEGURIDAD FÍSICA Y AMBIENTAL.	31%	31%
A.12	SEGURIDAD EN LA OPERATIVA.	8%	53%
A.13	SEGURIDAD EN LAS TELECOMUNICACIONES.	23%	23%
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	12%	70%
A.15	RELACIONES CON SUMINISTRADORES.	4%	4%
A.16	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	1%	90%
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	5%	90%
A.18	CUMPLIMIENTO.	25%	81%

Tabla 34. Evolución del Cumplimiento ISO/IEC 27002 Agrupada por Dominios

4. Presentación de Resultados

La figura siguiente muestra la situación global de los niveles de madurez en la que se encuentran los controles de la Norma ISO/IEC 27002. Es necesario resaltar que aún después de la implantación de los proyectos el 50% de los controles de la norma permanecen aún en los niveles L0 y L1, es decir, una efectividad entre el 0% y el 10% respectivamente.

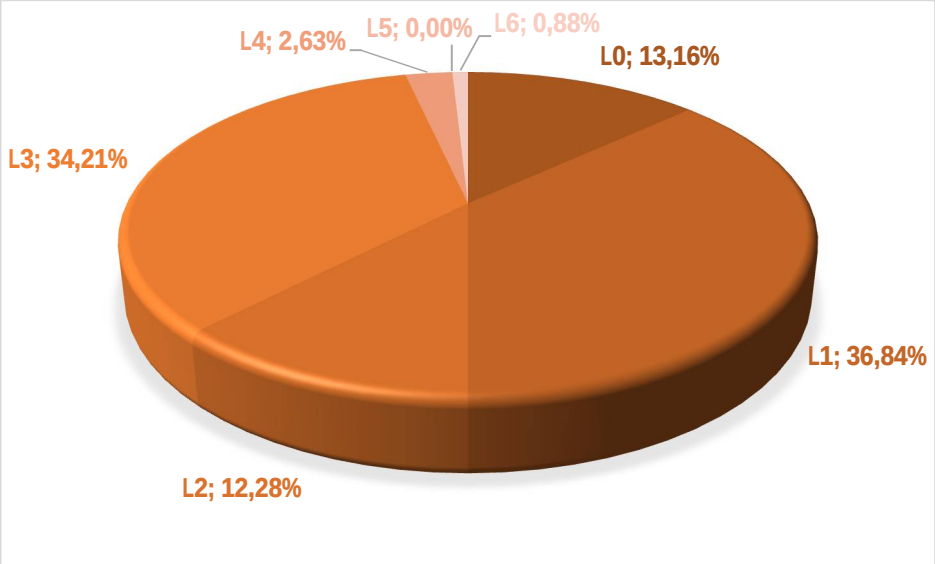


Ilustración 15. Porcentaje de Controles por Nivel de Madurez

El siguiente diagrama presenta el nivel de madurez de cada uno de los 18 dominios de la Norma ISO/IEC 27002 después de la implantación de los proyectos, ofreciendo una idea clara de los dominios que necesitan ser mejorados en el futuro para un cumplimiento adecuado de la norma.

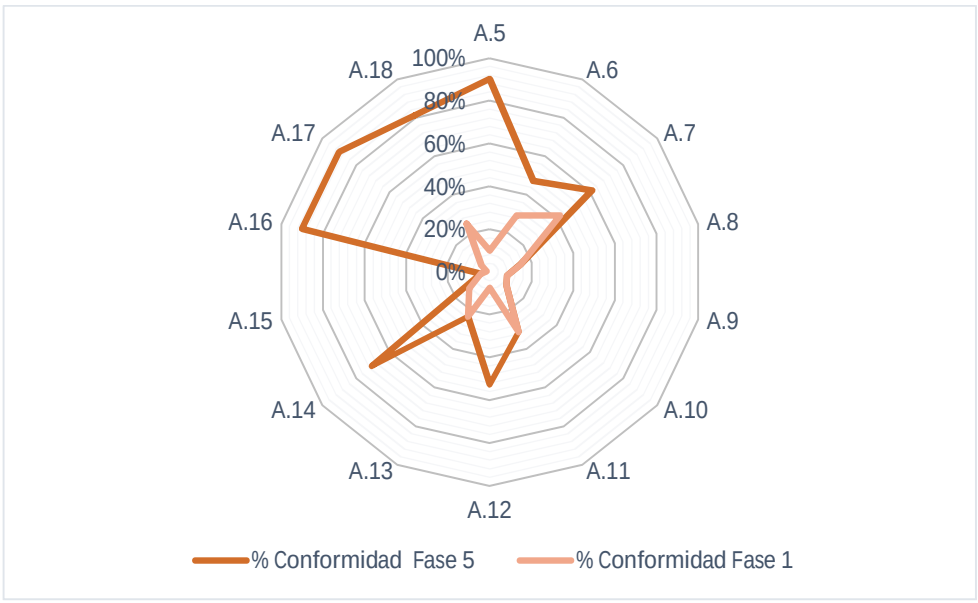


Ilustración 16. Porcentaje de Cumplimiento de los Controles por Dominios

5. No Conformidades ISO/IEC 27002

A continuación se muestra un resumen, clasificado por dominios, de la situación de las no conformidades del sistema auditado. Todos aquellos dominios con un valor mayor de 0 en la columna **"#NC Baja efectividad**" deberían ser abordados mediante acciones correctivas para un cumplimiento adecuado de la norma.

El ANEXO XIII incluye una ficha para cada objetivo de control de la norma ISO/27002 que para el que se ha detectado alguna no conformidad durante la auditoría.

	Dominio	% de conformidad	# NC baja efectividad	# NC alta efectividad	# NC OK
A.5	POLÍTICAS DE SEGURIDAD	90%	0	2	0
A.6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.	47%	2	4	1
A.7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	61%	1	2	2
A.8	GESTIÓN DE ACTIVOS.	15%	9	1	0
A.9	CONTROL DE ACCESOS.	8%	14	0	0
A.10	CIFRADO.	10%	2	0	0
A.11	SEGURIDAD FÍSICA Y AMBIENTAL.	31%	7	8	0
A.12	SEGURIDAD EN LA OPERATIVA.	53%	8	6	0
A.13	SEGURIDAD EN LAS TELECOMUNICACIONES.	23%	5	2	0
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	70%	3	10	0
A.15	RELACIONES CON SUMINISTRADORES.	4%	5	0	0
A.16	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	90%	0	7	0
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	90%	0	4	0
A.18	CUMPLIMIENTO.	81%	1	7	0
	Total		57	53	3

Tabla 35. No Conformidades Agrupadas por Dominios

6. Conclusiones

La ilustración 16 muestra un avance sustancial en cuanto a los niveles de cumplimiento de muchos de los dominios de la Norma ISO/IEC 27002. Los logros que se obtendrían serían fruto de la implantación de los proyectos propuestos. Estas propuestas han sido derivadas del análisis de riesgos a los que está sometido el sistema en cuestión. A pesar de la implantación de todos los proyectos algunos de los dominios no consiguen una mejora apreciable. Esto es debido a que ninguno de ellos afecta a los controles incluidos en dichos dominios. Es por esta razón que se ha realizado la auditoría de cumplimiento de la Norma IOS/IEC 27002, con el objeto de identificar los no cumplimientos tras la implantación de los proyectos y la ejecución de este plan director, poniendo de manifiesto las deficiencias de la organización respecto de la norma.

Los proyectos propuestos sugieren una **mejora sustancial** en los dominios **A5. Políticas de Seguridad**, **A.16. Gestión de Incidentes en la Seguridad de la Información y A.17. Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio**. Provocarían una **mejora moderada, aunque suficiente** (Nivel L2: Proceso Gestionado) en los dominios **A7. Seguridad ligada a los Recursos Humanos**, **A.12. Seguridad en la Operativa**, **A.14. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información** y **A.18. Cumplimiento Legal**. Se obtiene una **mejora por debajo del nivel esperado L2** (sólo se llega al Nivel L1: Proceso Ejecutado) en los dominios **A.6. Aspectos Organizativos de la Seguridad de la Información**, **A.8. Gestión de Activos**, **A.10. Cifrado**, **A.11. Seguridad Física y Ambiental**, **A.13. Seguridad de las Telecomunicaciones**. Por último, no se obtiene ninguna mejora en los Dominios **A.9. Control de Accesos** y **A.15. Relaciones con Suministradores**.

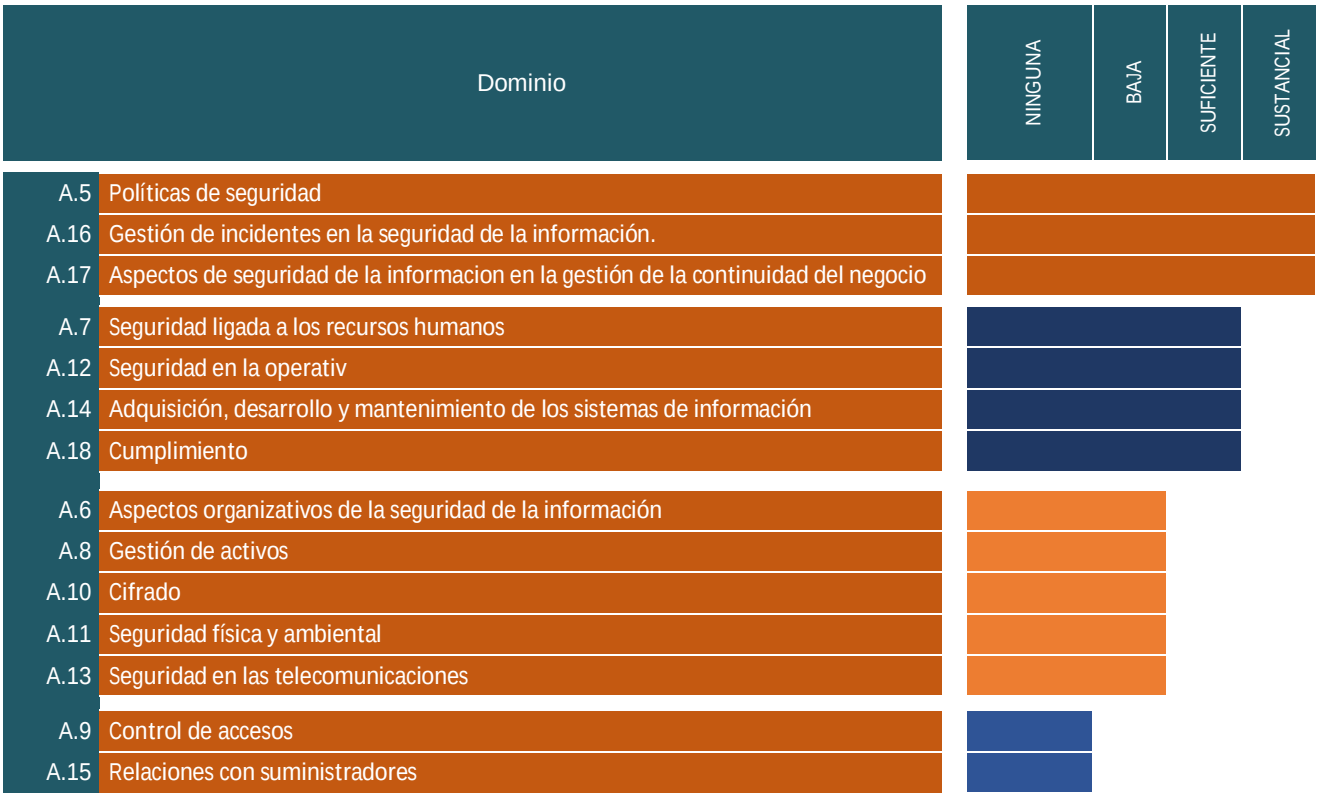


Ilustración 17. Mejora experimentanda por cada dominio después del proyecto

Es importante tener en cuenta que como muestra la ilustración 15, el 50% de los controles evaluados están en un nivel L0 o L1, es decir, con una efectividad entre El 0% y el 10% y aunque no es uno de los objetivos contemplados en este plan director de la seguridad de la información, el abordaje de las no conformidades expuestas en el "***Anexo XIII. No conformidades con la norma ISO 27002:2013***", después de la implantación de este plan sería el inicio del camino que podría llevar a la organización a la certificación ISO/IEC 27001.

Por otro lado, cabe destacar la aplicación de las Guías SAFER al proyecto, metodología para la evaluación de los Sistemas de Información en relación con la Seguridad del Paciente. Esta metodología persigue la mejora continua de los Sistemas de Información Sanitarios en cuanto a su desarrollo y adquisición, uso por parte de los profesionales, y supervisión y monitorización por la organización. Es de esperar un importante crecimiento de la mejora de la calidad y la seguridad de la información y la seguridad del paciente en el futuro gracias a la aplicación de esta metodología.

ANEXOS

7. Anexo I. Análisis diferencial detallado del sistema de urgencias respecto de la ISO/IEC 27001

Se ha realizado el análisis diferencial respecto de los dominios establecidos para la ISO/IEC 27001. En la Fase I de este documento se ha presentado un resumen de los resultados de dicho análisis que se puede sintetizar en la figura siguiente:

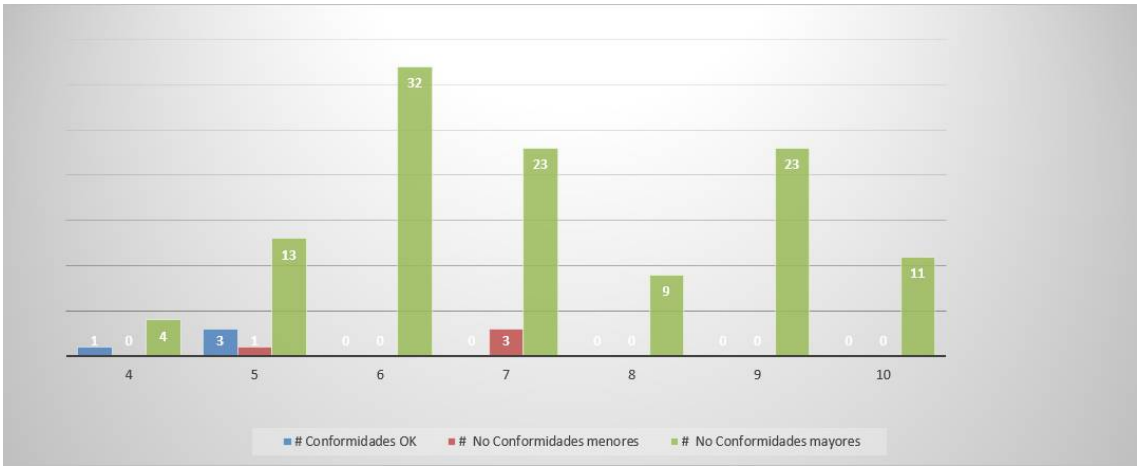


Ilustración 18 Gráfico de cumplimiento ISO/IEC 27001

Para consultar el detalle de los cálculos realizados para cada dominio se puede ver el documento ***Anexo_1_Analisis Diferencial_ISO_27001_2013.xlsx.*** Esta figura ya indica por si sóla que hay un ámplio margen de mejora para la implantación de la ISO/IEC 27001

8. Anexo II. Análisis diferencial detallado del sistema de urgencias respecto de la ISO/IEC 27002

El documento ***Anexo_2_Analisis Diferencial_ISO_27002_2013.xlsx*** contiene el análisis diferencial detallado para cada uno de los dominios y controles de la ISO/IEC 27002. El análisis realizado arroja los datos mostrados por la figura resumen siguiente:

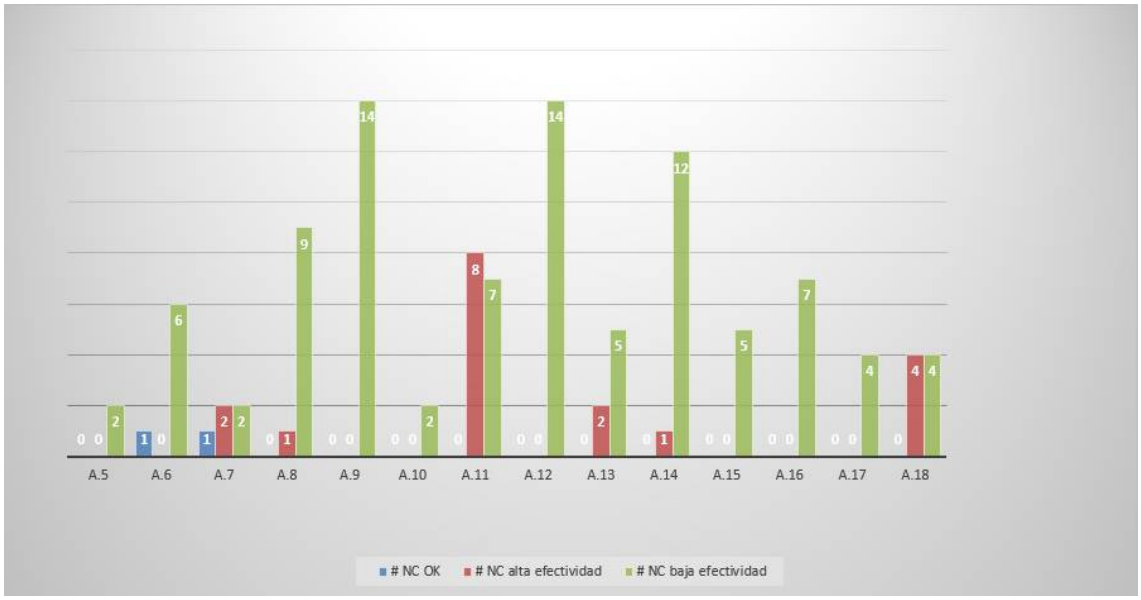


Ilustración 19. Gráfico de Cumplimiento de ISO/IEC 27002 por dominios

Esta figura ya indica por si sóla que hay un ámplio margen de mejora para la implantación de la ISO/IEC 27002

9. Anexo III. Politica de Seguridad.

La política de seguridad de la información establece los principios y líneas de actuación globales en cuestiones de seguridad de la información, alineados con los objetivos de la organización.

La política debe demostrar el compromiso de la Dirección con la seguridad de la información y se debe dar a conocer a todos los usuarios.

La política de seguridad de la información se desarrolla y concreta en políticas, normas, guías y estándares de segundo nivel.

Para el Servicio de Atención en Urgencias del Complejo Hospitalario Provincial son aplicables las siguientes políticas de seguridad de la información:

- La política de seguridad de la información de la junta de Andalucía recogida en la RESOLUCIÓN de 27 de septiembre de 2004, de la Secretaría General para la Administración Pública, por la que se establece el manual de comportamiento de los empleados públicos en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía
- DECRETO 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.
- Las políticas de seguridad de la información Corporativas recogidas en los siguientes documentos:
    - Documento de Seguridad de la Información Corporativa.
    - Resolución 23/2001. Instrucciones sobre procedimiento de acceso de usuarios a la documentación clínica y sobre procedimiento para garantizar la continuidad documental.
    - Resolución 184/2003 corporativa de instrucciones sobre el procedimiento de ordenación y gestión de la documentación clínica en centros asistenciales.
    - Las políticas de seguridad recogidas en el Reglamento de la Historia Clínica Electrónica del Complejo Hospitalario.

El documento *01 - 01 DocumentoPolíticasSeguridad.pdf* es el documento que detalla todas las políticas aplicables al Complejo Hospitalario Provincial y por tanto al Servicio de Atención en Urgencias.

El Documento de políticas de seguridad incluye además los siguientes anexos:

- Procedimiento operativo Gestión de las Operaciones y las Comunicaciones (POE-SGSI-0102)
- Procedimiento operativo de Gestión de la Continuidad del Negocio (POE-SGSI- 0103)
- Procedimiento operativo Gestión de Control de Accesos (POE-SGSI-0104)
- Procedimiento operativo de Compra Desarrollo Mantenimiento Sistemas (POE-SGSI-0105)
- Procedimiento operativo de Gestión de la Seguridad Física (POE-SGSI-0106)
- Procedimiento operativo de Gestión de no Conformidades y Acciones Correctoras (POE-SGSI -0107)
- Procedimiento operativo estandarizado de Gestión de la Formación (POE-SGSI-0108)

- Manual de Documentación (MN-SGSI-0109)

10. Anexo IV. Procedimiento de Auditoría del Sistema de Gestión de La Seguridad de la Información

El objetivo de este procedimiento es describir los procesos establecidos por el Complejo Hospitalario Provincial para la planificación, elaboración y documentación de las auditorías internas del SGSI, y definir las responsabilidades asociadas.

También describe la operativa descrita por este Hospital para planificar e implementar el proceso de auditorías del Sistema de Gestión de Seguridad necesario para:

- asegurar la conformidad del Sistema con las normas de referencia,
- mejorar continuamente la eficacia del Sistema.

Este procedimiento es de aplicación a todas las actividades, productos y servicios del Servicio de Urgencias del Complejo Hospitalario Provincial que puedan tener alguna influencia en los procesos descritos en el alcance del plan de Sistemas de Gestión de Seguridad de la Información del Servicio de Urgencias del Complejo Hospitalario Provincial

El procedimiento de auditoría describe los aspectos siguientes

- REQUISITOS GENERALES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.
    - Equipo auditor
- PROCEDIMIENTO DE ACTUACIÓN PARA AUDITORÍAS INTERNAS
    - Planificación de la auditoría
    - Desarrollo de la auditoría
    - Documentación de los resultados
    - Seguimiento de acciones correctivas
- Registros del Sistema de Gestión de Seguridad de la Información.

Puede encontrarse el documento completo en *02 - 01 - ProcedimientoAuditoríaSGSI.pdf* (**POE - SGSI - 0201)**

11. Anexo V. Indicadores del SGSI

ID	CONTROL	INDICADOR	DESCRIPCIÓN	FÓRMULA	TOLERANCIA	FRECUENCIA
1	5.1.2	Política de Seguridad (IND-001)	Revisión de la política por parte de la dirección	Al menos 1 vez al año se verifica la revisión de las políticas	=1	Anual
2	6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.1.5	Organización Interna (IND-002)	Verificación de los aspectos: • Las responsabilidades del SGSI están definidas y asignadas • Las tareas están segregadas • Están definidas las personas que mantienen los contactos con las autoridades • Los proyectos desarrollados incorporan la seguridad de la información	Número de NO conformidades detectadas en estos controles en la última auditoria.	No debe superar 1. (0 <= IND-002 <=1)	Anual
3	6.2.1	Movilidad (IND-003)	Se respetan las políticas de movilidad	Nº Dispositivos Móviles asegurados / Nº dispositivos móviles totales *100	> =90% (90% <= IND-003 <= 100%)	Anual
4	6.2.2	Teletrabajo (IND-004)	Se respetan las políticas de teletrabajo	Nº Conexiones VPN/ Nº Conexiones Totales * 100	>= 95% (95% <= IND-004 <= 100%)	Anual
5	7.1.2	Antes de Contratación (IND-005)	El nuevo trabajador firma Términos y Condiciones de la contratación	Nº Documentos Firmados/Nº Contratos totales * 100	>=99% (99% <= IND-004 <= 100%)	Anual
6	7.2.2.	Durante la Contratación (IND-006)	Los trabajadores han recibido formación y están concienciados con la seguridad de la información	Nº trabajadores con formación/ Nº trabajadores totales * 100	Año 1 IND-006 >= 70% Año 2 IND-006 >= 85%	Anual

ID	CONTROL	INDICADOR	DESCRIPCIÓN	FÓRMULA	TOLERANCIA	FRECUENCIA
					Año 3 IND-006 = 100%	
7	7.3.1.	Cese (IND-007)	Se han comunicado las obligaciones al trabajador antes de su cese o cambio de puesto de trabajo	Nº comunicaciones / Nº ceses y cambios totales * 100	> 90% (90% <= IND-007 <= 100%)	Anual
8	8.1.1	Inventario (IND-008)	Se verifica que los equipos inventariados están en su sitio	Nº de equipos correctos / Nº equipos totales * 100	>=95% (95% <= IND-008 <= 100%)	Anual
9	8.2.2.	Etiquetado Información (IND-009)	Se verifica que la información en papel está correctamente etiquetada	AZ Correctamente etiquetados/ AZ totales * 100	>=90% (90% <= IND-009 <= 100%)	Bienal
10	9.2.1.	Altas y Bajas Usuarios (IND-010)	Se comprueba que el registro de usuarios se corresponde con los usuarios realmente activos en el sistema	Nº Usuarios activos / Nº usuarios con acceso al sistema * 100	>95% (95% <= IND-010 <= 100%)	Anual
11	10.1.1.	Cifrado (IND-011)	Verificación de que los procesos que tratan con datos sensibles han implantado totalmente controles criptográficos apropiados	Nº Tratamientos Cifrados /Nº Tratamientos totales identificados sensibles * 100	>95% (95% <= IND-011 <= 100%)	Anual
12	11.1	Áreas Seguras (IND-012)	Verificación de que se aplican las medidas correctoras propuestas en las auditorías anteriores	Nº Medidas correctoras aplicadas / Nº Medidas correctoras propuestas totales * 100	>95% (95% <= IND-012 <= 100%)	Anual
13	12.1	Seguridad Operativa (IND-013)	Verificación de la madurez de los procesos de TI para los procesos de Gestión de cambios, Gestión de Capacidades, Separación de Entornos	Todos los procesos deben superar el nivel 1 (Proceso Ejecutado. Cumple con su objetivo)	>=1 (1 <= IND-013 <= 5)	Anual
14	12.3.1	Restauración	Verificación de copias de seguridad exitosas dos	(>=2)	>=2	Anual

ID	CONTROL	INDICADOR	DESCRIPCIÓN	FÓRMULA	TOLERANCIA	FRECUENCIA
		(IND-014)	veces al año	Nº de restauraciones exitosas	(2 <= IND-014 <= 12)	
15	13.2	Comunicaciones Externas (IND-015)	Verificación de que las comunicaciones externas (con profesionales o terceras partes) cumplen con las medidas de seguridad establecidas en la política	Nº Comunicaciones externas protegidas /Nº comunicaciones externas totales * 100	>90% (90% <= IND-015 <= 100%)	Anual
16	14.3.1	Datos de Prueba (IND-016)	Las aplicaciones en desarrollo o prueba sólo utilizan datos de prueba y en ningún caso copias de los datos reales.	Nº aplicaciones en prueba con datos de prueba / Nº Total aplicaciones en pruebas * 100	>90% (90% <= IND-016 <= 100%)	Anual
17	15.1	Prestación del Servicio (IND-017)	Revisión periódica de los acuerdos de nivel de servicio	Nº incumplimientos SLA / Nº total SLA * 100	< 10% (10% >= IND-017 >= 0%)	Anual
18	16.1.4	Respuesta Incidentes (IND-018)	Se evalúan y se responde a los incidentes comunicados	Nº Incidentes evaluados / Nº incidentes comunicados * 100%	>90% (90% <= IND-018 <= 100%)	Anual
19	A.17.1	Continuidad del Negocio (IND-019)	Se han probado los planes de continuidad del negocio con éxito	Nº planes contingencias probados / Nº planes totales	>90% (90% <= IND-019 <= 100%)	Bienal
20	18.1.	Auditorías LOPD (IND-020)	Se verifica el cumplimiento legal con la LOPD mediante auditoría independiente	Se hace auditoría LOPD bienal	>=1 (1 <= IND-020 <= 2)	Bienal

ID	CONTROL	INDICADOR	DESCRIPCIÓN	FÓRMULA	TOLERANCIA	FRECUENCIA
21	N/A	Autoevaluación SAFER (IND-021)	Se realiza autoevaluación de las guías SAFER	Se realiza autoevaluación y se envía informe a la dirección y CSI	>=1 (1 <= IND-020 <= 2)	Bienal

12. Anexo VI. Procedimiento de Revisión por la Dirección

Este procedimiento define la metodología utilizada para la revisión del Sistema de Gestión de Seguridad de la Información (SGSI) en el Servicio de Urgencias del Complejo Hospitalario Provincial por parte de la dirección del centro. Este procedimiento garantiza información actualizada al equipo directivo respecto de los riesgos y necesidades del SGSI regularmente.

Se definen los responsables de la revisión del SGSI, el proceso de revisión y los informes que serán revisados:

- Informes previos de revisión por la dirección.
- Informes de cambios internos o externos relevantes en referencia al SGSI
- Informe de Rendimiento del SGSI:
    - Resultados de auditorías del SGSI
    - Cuadro de control de indicadores
    - Informe de Objetivos de Seguridad Alcanzados
- Informe de oportunidades de mejora
- Informe de modificaciones del plan de gestión del riesgo

Por último se define al Responsable de Seguridad de la Información quien se encargará de presentar los resultados a la dirección.

Se puede consultar el documento completo en *04 - 01 - ProcedimientoRevisionDireccion* (**POE - SGSI - 0401)**

13. Anexo VII. Gestión de Roles y Responsabilidades

Este procedimiento establecer la estructura básica del Comité de Seguridad de la Información a modo de norma para su utilización como guía en la formalización de dicho comité.

El presente documento cubre las siguientes áreas ISO 27002:

- 6.1.1. Compromiso de la Dirección con la Seguridad de la Información
- 6.1.2. Coordinación de la Seguridad de la Información

Definir una estructura de seguridad implica tomar decisiones sobre las líneas de actuación a desarrollar y la implantación de medidas concretas en cada una de dichas líneas. Generalmente estas decisiones abarcan a todos los departamentos de la organización, jurídico, organizativo, recursos humanos y personal, calidad, etc., de esta forma, las actuaciones en materia de seguridad deben desarrollarse de forma estructurada y con el mayor consenso y colaboración posible.

Es conveniente generar un grupo de trabajo en la organización para debatir y adoptar las principales iniciativas en materia de seguridad de la información.

La dirección debe crear el comité de seguridad y asignar los puestos que deben ocupar en su distribución los diferentes departamentos de la organización. También resulta de especial importancia crear un canal fluido para enviar a la dirección las decisiones acordadas en el comité de seguridad.

En este procedimiento se establecen los siguientes aspectos:

- Personal involucrado en la norma
  - Miembros
  - Funciones
- Formalización del Comité de Seguridad de la Información
  - Reglamento interno de trabajo
  - Normas de funcionamiento y organización

Se puede consultar el documento completo en *05 - 01 - Gestion de Roles y Responsabilidades. pdf* (**POE - SGSI - 0501)**

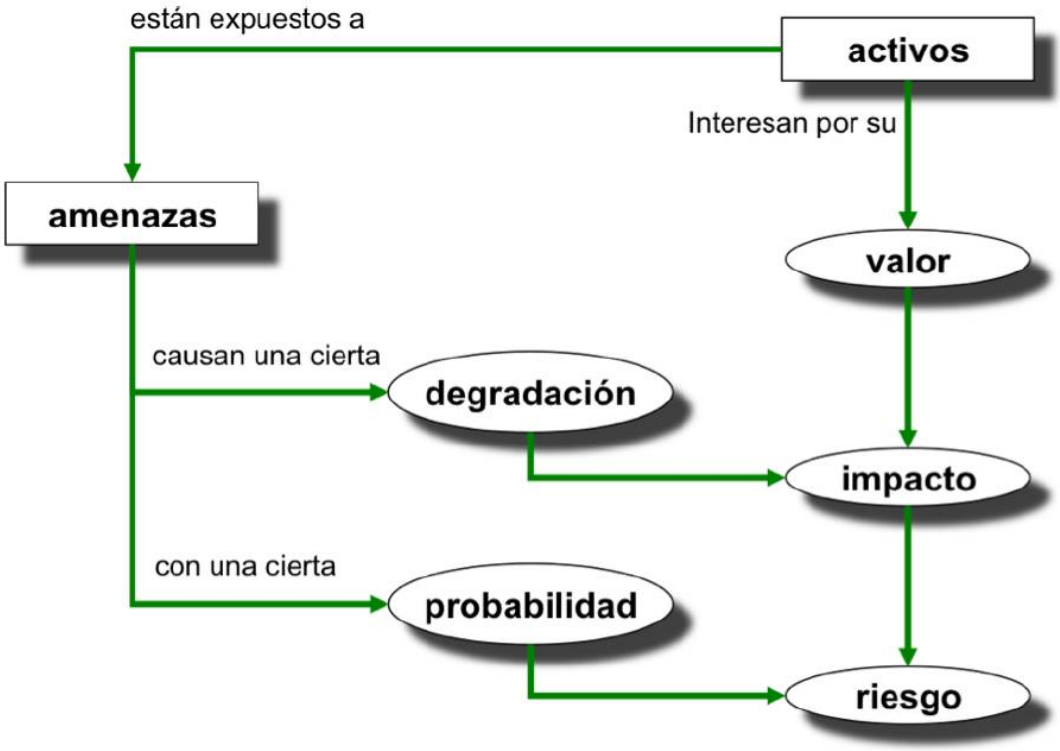
14. Anexo VIII: Metodología de Análisis de Riesgos

El Análisis de Riesgos consiste en identificar y valorar los riesgos a los que están sometidos los activos de nuestro sistema. Los pasos a seguir en el Análisis de Riesgo son los siguientes:

- determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
- determinar a qué amenazas están expuestos aquellos activos
- determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
- estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
- estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza

Con el objeto de organizar la presentación, se introducen los conceptos de —impacto y riesgo potenciales entre los pasos 2 y 3. Estas valoraciones son ”teóricas” en el caso de que no hubiera salvaguarda alguna desplegada. Una vez obtenido este escenario teórico, se incorporan las salvaguardas del paso 3, derivando estimaciones realistas de impacto y riesgo.

Cada una de estas etapas se muestra en el esquema de la página siguiente.



El proceso de análisis y gestión de riesgos de Magerit v3.0 se resumen en lo siguiente:

- Paso 1: Identificación y valoración de Activos
- Paso 2: Identificación de Amenazas.
    - Determinación del impacto potencial
    - Determinación del riesgo potencial
- Paso 3: Salvaguardas
- Paso 4: impacto residual
- Paso 5: riesgo residual
- Gestión del Riesgo
    - Elaboración del Plan del Riesgo
    - Asignación de Responsabilidades
- Actualización y Seguimiento del Plan de Riesgo
- Elaboración del plan de Implantación de los Controles
    - Definición de la Planificación
    - Descripción de las Tareas a Realizar
    - Definición y Seguimiento de Indicadores

Se puede consultar el procedimiento detallado en el documento *06 - 01 - ProcedimientoAnalisisYGestionRiesgos* (**POE - SGSI - 0601)**

15. Anexo VIII. Declaración de Aplicabilidad

REF.	Control	Aplica SI/NO	Aplicabilidad	Procesos/Documentos	Indicador	Estado
A.5 POLÍTICAS DE SEGURIDAD A.5.1 Directrices de la Dirección en seguridad de la información						
A.5.1.1	Conjunto de políticas para la seguridad de la información	SI	Se debería definir un conjunto de políticas para la seguridad de la información, aprobado por la dirección, publicado y comunicado a los empleados así como a todas las partes externas relevantes.	• Política de Seguridad (Anexo I)	NO	L1
A.5.1.2	Revisión de las políticas para la seguridad de la información	SI	Las políticas para la seguridad de la información se deberían planificar y revisar con regularidad o si ocurren cambios significativos para garantizar su idoneidad, adecuación y efectividad.	• Acta de Comisión de Seguridad de la Información • Informe de Revisión de Dirección	(IND-001)	L1
A.6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INF. A.6.1 Organización interna						
A.6.1.1	Asignación de responsabilidades para la seguridad de la información.	SI	Se deberían definir y asignar claramente todas las responsabilidades para la seguridad de la información	• Actas de Nombramiento Comisión de Seguridad de la Información	(IND-002)	L1
A.6.1.2	Segregación de tareas.	SI	Se deberían segregar tareas y las áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización	• Actas Comisión de Seguridad de la Información	(IND-002)	L0

REF.	Control	Aplica SI/NO	Aplicabilidad	Procesos/Documentos	Indicador	Estado
A.6.1.3	Contacto con las autoridades	SI	Se deberían mantener los contactos apropiados con las autoridades pertinentes	• Actas de Nombramiento Comisión de Seguridad de la Información	(IND-002)	L1
A.6.1.4	Contacto con grupos de interés especial	SI	Se debería mantener el contacto con grupos o foros de seguridad especializados y asociaciones profesionales.	• Actas reuniones/certificaciones asistencia foros especializados	(IND-002)	L1
A.6.1.5	Seguridad de la información en la gestión de proyectos	SI	Se debería contemplar la seguridad de la información en la gestión de proyectos e independientemente del tipo de proyecto a desarrollar por la organización.	• Actas de Nombramiento Comisión de Seguridad de la Información	(IND-002)	L0
A.6.2	Dispositivos para movilidad y teletrabajo.					
A.6.2.1	Política de uso de dispositivos para movilidad.	SI	Se debería establecer una política formal y se deberían adoptar las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones.	• Política de Seguridad (Anexo I)	(IND-003)	L1
A.6.2.2	Teletrabajo.	SI	Se debería desarrollar e implantar una política y medidas de seguridad de apoyo para proteger a la información accedida, procesada o almacenada en ubicaciones destinadas al teletrabajo	Política de Seguridad (Anexo I)	(IND-004)	L4
A.7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.					
A.7.1	Organización interna					
A.7.1.1	Investigación de antecedentes.	NO	Se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los	• N/A	NO	L6

REF.	Control	Aplica SI/NO	Aplicabilidad	Procesos/Documentos	Indicador	Estado
			riesgos percibidos.			
A.7.1.2	Términos y condiciones de contratación.	SI	Como parte de su obligación contractual, empleados, contratistas y terceros deberían aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.	• Política de Seguridad (Anexo I) • Contratos	(IND-005)	L4
A.7.2	Durante la contratación.					
A.7.2.1	Responsabilidades de gestión.	SI	La Dirección debería requerir a empleados, contratistas y usuarios de terceras partes aplicar la seguridad en concordancia con las políticas y los procedimientos	• Auditorías de terceros.	(IND-005)	L1
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	SI	Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	• Plan de formación / concienciación en protección de datos y seguridad de la información.	(IND-006)	L3
A.7.2.3	Proceso disciplinario.	SI	Debería existir un proceso formal disciplinario comunicado a empleados que produzcan brechas en la seguridad.	• Política de Seguridad (POL) (Anexo I)	NO	L3
A.7.3	Cese o cambio de puesto de trabajo.					
A.7.3.1	Cese o cambio de puesto de trabajo.	SI	Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste deberían estar claramente definidas, comunicadas a empleado o contratista y asignadas efectivamente.	• Política de Seguridad (POL) (Anexo I)	(IND-007)	L0

REF.	Control	Aplica SI/NO	Aplicabilidad	Procesos/Documentos	Indicador	Estado
A.8	GESTIÓN DE ACTIVOS.					
A.8.1	Responsabilidad sobre los activos.					
A.8.1.1	Inventario de activos.	SI	Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.	• Inventario de activos	(IND-008)	L1
A.8.1.2	Propiedad de los activos.	SI	Toda la información y activos del inventario asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.	• Inventario de activos	NO	L1
A.8.1.3	Uso aceptable de los activos.	SI	Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.	• Política de Seguridad (Anexo I)	NO	L3
A.8.1.4	Devolución de activos.	SI	Todos los empleados y usuarios de terceras partes deberían devolver todos los activos de la organización que estén en su posesión/responsabilidad una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo.	• Política de Seguridad (Anexo I)	NO	L0
A. 8.2 Clasificación de la información						
A.8.2.1	Directrices de clasificación.	SI	La información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.	• Manual de Documentación	NO	L1
A.8.2.2	Etiquetado y manipulado de la información.	SI	Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el	• Manual de Documentación	(IND-009)	L1

REF.	Control	Aplica SI/NO	Aplicabilidad	Procesos/Documentos	Indicador	Estado
			esquema de clasificación adoptado por la organización.			
A.8.2.3	Manipulación de activos.	SI	Se deberían desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización.	• Política de Seguridad (Anexo I)	NO	L1
A.8.3	Manejo de los soportes de almacenamiento.					
A.8.3.1	Gestión de soportes extraíbles.	SI	Se deberían establecer procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la organización	• Política de Seguridad (Anexo I)	NO	L1
A.8.3.2	Eliminación de soportes.	SI	Se deberían eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales	• Política de Seguridad (Anexo I)	NO	L1
A.8.3.3	Soportes físicos en tránsito	NO	Se deberían proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.	Política de Seguridad (Anexo I)	NO	L0
A.9	CONTROL DE ACCESOS.					
A.9.1	Requisitos de negocio para el control de accesos.					
A.9.1.1	Política de control de accesos.	SI	Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización	• Gestión de Control de Accesos	NO	L1

REF.	Control	Aplica SI/NO	Aplicabilidad	Procesos/Documentos	Indicador	Estado
A.9.1.2	Control de acceso a las redes y servicios asociados.	SI	Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar	• Gestión de Operaciones y Comunicaciones	NO	L1
A.9.2 Gestión de acceso de usuario.						
A.9.2.1	Gestión de altas/bajas en el registro de usuarios.	SI	Debería existir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso	• Gestión de Control de Accesos	(IND-010)	L1
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios.	SI	Se debería de implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.	• Gestión de Control de Accesos	NO	L1
A.9.2.3	Gestión de los derechos de acceso con privilegios especiales.	SI	La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado.	• Gestión de Control de Accesos	NO	L0
A.9.2.4	Gestión de información confidencial de autenticación de usuarios.	SI	La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado.	• Gestión de Control de Accesos	NO	L0
A.9.2.5	Revisión de los derechos de acceso de los usuarios.	SI	Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.	• Gestión de Control de Accesos	NO	L0
A.9.2.6	Retirada o adaptación de los derechos de acceso	SI	Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio	• Gestión de Control de Accesos	NO	L0

REF.	Control	Aplica SI/NO	Aplicabilidad	Procesos/Documentos	Indicador	Estado
A.9.3	Responsabilidades del usuario.					
A.9.3.1	Uso de información confidencial para la autenticación.	SI	Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación.	• Política de Seguridad (Anexo I)	NO	L1
A.9.4	Control de acceso a sistemas y aplicaciones.					
A.9.4.1	Restricción del acceso a la información.	SI	Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.	• Gestión de Control de Accesos	NO	L1
A.9.4.2	Procedimientos seguros de inicio de sesión.	SI	Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on	• Gestión de Control de Accesos	NO	L1
A.9.4.3	Gestión de contraseñas de usuario.	SI	Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad.	• Gestión de Control de Accesos	NO	L1
A.9.4.4	Uso de herramientas de administración de sistemas.	SI	El uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas deberían estar restringidos y estrechamente controlados.	• Política de Seguridad (Anexo I)	NO	L1
A.9.4.5	Control de acceso al código fuente de los programas.	SI	Se debería restringir el acceso al código fuente de las aplicaciones software.	• Gestión de Control de Accesos	NO	L1
A.10 A.10.1	CIFRADO. Controles criptográficos.					
A.10.1.1	Política de uso de los	SI	Se debería desarrollar e implementar una política que	• Política de Seguridad (Anexo I)	(IND-011)	L1

REF.	Control	Aplica SI/NO	Aplicabilidad	Procesos/Documentos	Indicador	Estado
	controles criptográficos.		regule el uso de controles criptográficos para la protección de la información	• Gestión de Operaciones y Comunicaciones		
A.10.1.2	Gestión de claves.	SI	Se debería desarrollar e implementar una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida	• Política de Seguridad (Anexo I) • Gestión de Operaciones y Comunicaciones	NO	L1
A.11 SEGURIDAD FÍSICA Y AMBIENTAL. A.11.1 Áreas seguras.						
A.11.1.1	Perímetro de seguridad física.	SI	Se deberían definir y utilizar perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica.	• Procedimiento de Gestión de la Seguridad Física	(IND-012)	L1
A.11.1.2	Controles físicos de entrada.	SI	Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso.	• Procedimiento de Gestión de la Seguridad Física	(IND-012)	L1
A.11.1.3	Seguridad de oficinas, despachos y recursos.	SI	Se debería diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización.	• Política de Seguridad (Anexo I) • Procedimiento de Gestión de la Seguridad Física	(IND-012)	L1
A.11.1.4	Protección contra las amenazas externas y ambientales.	SI	Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes.	• Gestión de la Continuidad del Negocio	(IND-012)	L2
A.11.1.5	El trabajo en áreas seguras.	SI	Se deberían diseñar y aplicar procedimientos para el desarrollo de trabajos y actividades en áreas seguras.	• Procedimiento de Gestión de la Seguridad Física	(IND-012)	L1
A.11.1.6	Áreas de acceso público,	SI	Se deberían controlar puntos de acceso a la organización como las áreas de entrega y	• Procedimiento de Gestión de la Seguridad Física	(IND-012)	L2

REF.	Control	Aplica SI/NO	Aplicabilidad	Procesos/Documentos	Indicador	Estado
	carga y descarga.		carga/descarga (entre otros) para evitar el ingreso de personas no autorizadas a las dependencias aislando estos puntos, en la medida de lo posible, de las instalaciones de procesamiento de información			
A.11.2	Seguridad de los equipos.					
A.11.2.1	Emplazamiento y protección de equipos.	SI	Emplazamiento y protección de equipos: Los equipos se deberían emplazar y proteger para reducir los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado	• Política de Seguridad (Anexo I) • Procedimiento de Gestión de la Seguridad Física	NO	L2
A.11.2.2	Instalaciones de suministro.	SI	Los equipos deberían estar protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo	• Gestión de la Continuidad del Negocio	NO	L3
A.11.2.3	Seguridad del cableado.	SI	Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger contra la intercepción, interferencia o posibles daños	• Procedimiento de Gestión de la Seguridad Física	NO	L1
A.11.2.4	Mantenimiento de los equipos.	SI	Los equipos deberían mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas.	• Gestión de la Continuidad del Negocio	NO	L2
A.11.2.5	Salida de activos fuera de las dependencias de la empresa.	SI	Los equipos, la información o el software no se deberían retirar del sitio sin previa autorización.	• Procedimiento de Gestión de la Seguridad Física	NO	L0
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	SI	Se debería aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos	• Procedimiento de Gestión de la Seguridad Física	NO	L0

REF.	Control	Aplica SI/NO	Aplicabilidad	Procesos/Documentos	Indicador	Estado
A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	SI	Se deberían verificar todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización.	• Política de Seguridad (Anexo I) • Gestión de Soportes	NO	L2
A.11.2.8	Equipo informático de usuario desatendido.	SI	Los usuarios se deberían asegurar de que los equipos no supervisados cuentan con la protección adecuada.	• Política de Seguridad (Anexo I)	NO	L2
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	SI	Se debería adoptar una política de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información.	• Política de Seguridad (Anexo I)	NO	L2
A.12 SEGURIDAD EN LA OPERATIVA. A.12.1 Responsabilidades y procedimientos de operación.						
A.12.1.1	Documentación de procedimientos de operación.	SI	Se deberían documentar los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten.	• Política de Seguridad (Anexo I) • Gestión de Operaciones y Comunicaciones	(IND-013)	L1
A.12.1.2	Gestión de cambios.	SI	Se deberían controlar los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información	• Gestión de Operaciones y Comunicaciones	(IND-013)	L0
A.12.1.3	Gestión de capacidades.	SI	Se debería monitorear y ajustar el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.	• Gestión de Operaciones y Comunicaciones	(IND-013)	L1

REF.	Control	Aplica SI/NO	Aplicabilidad	Procesos/Documentos	Indicador	Estado
A.12.1.4	Separación de entornos de desarrollo, prueba y producción.	SI	Los entornos de desarrollo, pruebas y operacionales deberían permanecer separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional.	• Gestión de Operaciones y Comunicaciones	(IND-013)	L1
A.12.2	Protección contra código malicioso.					
A.12.2.1	Controles contra el código malicioso.	SI	Evitar infecciones	• Gestión de Operaciones y Comunicaciones	NO	L1
A.12.3	Copias de seguridad.					
A.12.3.1	Copias de seguridad de la información.	SI	Se deberían realizar y pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.	• Gestión de la Continuidad del Negocio	(IND-014)	L1
A.12.4	Registro de actividad y supervisión.					
A.12.4.1	Registro y gestión de eventos de actividad.	SI	Se deberían producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.	• Gestión de Control de Accesos	NO	L0
A.12.4.2	Protección de los registros de información.	SI	Se debería proteger contra posibles alteraciones y accesos no autorizados la información de los registros.	• Gestión de Control de Accesos	NO	L1
A.12.4.3	Registros de actividad del administrador y operador del sistema.	SI	Se deberían registrar las actividades del administrador y del operador del sistema y los registros asociados se deberían proteger y revisar de manera regular.	• Gestión de Control de Accesos	NO	L0

REF.	Control	Aplica SI/NO	Aplicabilidad	Procesos/Documentos	Indicador	Estado
A.12.4.4	Sincronización de relojes.	SI	Se deberían sincronizar los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o de un dominio de seguridad y en relación a una fuente de sincronización única de referencia.	• Gestión de Operaciones y Comunicaciones	NO	L1
A.12.5	Control del software en explotación.					
A.12.5.1	Instalación del software en sistemas en producción.	SI	Se deberían implementar procedimientos para controlar la instalación de software en sistemas operacionales.	• Gestión de Operaciones y Comunicaciones	NO	L1
A.12.6	Gestión de la vulnerabilidad técnica.					
A.12.6.1	Gestión de las vulnerabilidades técnicas.	SI	Se debería obtener información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna para evaluar el grado de exposición de la organización y tomar las medidas necesarias para abordar los riesgos asociados.	• Gestión de no conformidades y acciones correctoras	NO	L1
A.12.6.2	Restricciones en la instalación de software.	SI	Se deberían establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.	• Procedimiento de Compra, Desarrollo y Mantenimiento	NO	L1
A.12.7	Consideraciones de las auditorías de los sistemas de información.					
A.12.7.1	Controles de auditoría de los sistemas de información.	SI	Se deberían planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.	• Gestión de Operaciones y Comunicaciones	NO	L0

REF.	Control	Aplica SI/NO	Aplicabilidad	Procesos/Documentos	Indicador	Estado
A.13	SEGURIDAD EN LAS TELECOMUNICACIONES.					
A.13.1	Gestión de la seguridad en las redes.					
A.13.1.1	Controles de red.	SI	Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.	• Gestión de Operaciones y Comunicaciones		L2
A.13.1.2	Mecanismos de seguridad asociados a servicios en red.	SI	Se deberían identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados.	• Gestión de Operaciones y Comunicaciones		L2
A.13.1.3	Segregación de redes.	NO	Se deberían segregar las redes en función de los grupos de servicios, usuarios y sistemas de información.	• Gestión de Operaciones y Comunicaciones		L1
A.13.2	Intercambio de información con partes externas.					
A.13.2.1	Políticas y procedimientos de intercambio de información.	SI	Deberían existir políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación.	• Gestión de Operaciones y Comunicaciones	(IND-015)	L1
A.13.2.2	Acuerdos de intercambio.	SI	Los acuerdos deberían abordar la transferencia segura de información comercial entre la organización y las partes externas	• Gestión de Operaciones y Comunicaciones	(IND-015)	L1
A.13.2.3	Mensajería electrónica.	SI	Se debería proteger adecuadamente la información referida en la mensajería electrónica	• Gestión de Operaciones y Comunicaciones	(IND-015)	L1
A.13.2.4	Acuerdos de	SI	Se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de	• Política de Seguridad (Anexo I)	(IND-015)	L1

REF.	Control	Aplica SI/NO	Aplicabilidad	Procesos/Documentos	Indicador	Estado
	confidencialidad y secreto.		confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información.			
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.					
A.14.1	Requisitos de seguridad de los sistemas de información.					
A.14.1.1	Análisis y especificación de los requisitos de seguridad.	SI	Los requisitos relacionados con la seguridad de la información se deberían incluir en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes.	• Procedimiento Compra Desarrollo Mantenimiento Sistemas	NO	L0
A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.	SI	La información de los servicios de aplicación que pasan a través de redes públicas se debería proteger contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada.	• Gestión de Operaciones y Comunicaciones	NO	L1
A.14.1.3	Protección de las transacciones por redes telemáticas.	SI	La información en transacciones de servicios de aplicación se debería proteger para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción.	• Gestión de Operaciones y Comunicaciones	NO	L2
A.14.2	Seguridad en los procesos de desarrollo y soporte.					
A.14.2.1	Política de desarrollo seguro de software.	SI	Se deberían establecer y aplicar reglas para el desarrollo de software y sistemas dentro de la organización.	• Procedimiento Compra Desarrollo Mantenimiento Sistemas	NO	L0
A.14.2.2	Procedimientos de control de cambios en los sistemas.	SI	En el ciclo de vida de desarrollo se deberían hacer uso de procedimientos formales de control de cambios.	• Procedimiento Compra Desarrollo Mantenimiento Sistemas	NO	L1

REF.	Control	Aplica SI/NO	Aplicabilidad	Procesos/Documentos	Indicador	Estado
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	SI	Las aplicaciones críticas para el negocio se deberían revisar y probar para garantizar que no se han generado impactos adversos en las operaciones o en la seguridad de la organización.	• Procedimiento Compra Desarrollo Mantenimiento Sistemas	NO	L0
A.14.2.4	Restricciones a los cambios en los paquetes de software.	SI	Se deberían evitar modificaciones en los paquetes de software suministrados por terceros, limitándose a cambios realmente necesarios. Todos los cambios se deberían controlar estrictamente.	• Procedimiento Compra Desarrollo Mantenimiento Sistemas	NO	L1
A.14.2.5	Uso de principios de ingeniería en protección de sistemas.	SI	Se deberían establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información.	• Procedimiento Compra Desarrollo Mantenimiento Sistemas	NO	L0
A.14.2.6	Seguridad en entornos de desarrollo.	SI	Las organizaciones deberían establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.	• Procedimiento Compra Desarrollo Mantenimiento Sistemas	NO	L1
A.14.2.7	Externalización del desarrollo de software.	NO	La organización debería supervisar y monitorear las actividades de desarrollo del sistema que se hayan externalizado.	• Procedimiento Compra Desarrollo Mantenimiento Sistemas	NO	L1
A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	SI	Se deberían realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.	• Procedimiento Compra Desarrollo Mantenimiento Sistemas	NO	L1
A.14.2.9	Pruebas de aceptación.	SI	Se deberían establecer programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones	• Procedimiento Compra Desarrollo Mantenimiento Sistemas	NO	L1

REF.	Control	Aplica SI/NO	Aplicabilidad	Procesos/Documentos	Indicador	Estado
A.14.3	Datos de prueba.					
A.14.3.1	Protección de los datos utilizados en pruebas.	SI	Los datos de pruebas se deberían seleccionar cuidadosamente y se deberían proteger y controlar.	• Procedimiento Compra Desarrollo Mantenimiento Sistemas	(IND-016)	L1
A.15	RELACIONES CON SUMINISTRADORES.					
A.15.1	Seguridad de la información en las relaciones con suministradores.					
A.15.1.1	Política de seguridad de la información para suministradores.	SI	Se deberían acordar y documentar adecuadamente los requisitos de seguridad de la información requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas.	• Procedimiento Compra Desarrollo Mantenimiento Sistemas	(IND-017)	L1
A.15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.	SI	Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la organización.	• Procedimiento Compra Desarrollo Mantenimiento Sistemas	(IND-017)	L0
A.15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.	SI	Los acuerdos con los proveedores deberían incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.	• Procedimiento Compra Desarrollo Mantenimiento Sistemas	(IND-017)	L0
A.15.2	Gestión de la prestación del servicio por suministradores.					
A.15.2.1	Supervisión y revisión de los servicios prestados por terceros.	SI	Las organizaciones deberían monitorear, revisar y auditar la presentación de servicios del proveedor regularmente.	• Procedimiento Compra Desarrollo Mantenimiento Sistemas		L1

REF.	Control	Aplica SI/NO	Aplicabilidad	Procesos/Documentos	Indicador	Estado
A.15.2.2	Gestión de cambios en los servicios prestados por terceros.	SI	Se deberían administrar los cambios a la provisión de servicios que realizan los proveedores manteniendo y mejorando: las políticas de seguridad de la información, los procedimientos y controles específicos. Se debería considerar la criticidad de la información comercial, los sistemas y procesos involucrados en el proceso de reevaluación de riesgos.	• Procedimiento Compra Desarrollo Mantenimiento Sistemas		L0
A.16	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.					
A.16.1	Gestión de incidentes de seguridad de la información y mejoras.					
A.16.1.1	Responsabilidades y procedimientos.	SI	Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	• Gestión de Roles y Responsabilidades • Gestión de la Continuidad del Negocio	NO	L1
A.16.1.2	Notificación de los eventos de seguridad de la información.	SI	Los eventos de seguridad de la información se deberían informar lo antes posible utilizando los canales de administración adecuados.	• Política de Seguridad (Anexo I) • Gestión de Incidentes	NO	L0
A.16.1.3	Notificación de puntos débiles de la seguridad	SI	Se debería requerir anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización.	• Política de Seguridad (Anexo I) • Gestión de Incidentes	NO	L0
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.	SI	Se deberían evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.	• Gestión de Incidentes	(IND-018)	L0

REF.	Control	Aplica SI/NO	Aplicabilidad	Procesos/Documentos	Indicador	Estado
A.16.1.5	Respuesta a los incidentes de seguridad.	SI	Se debería responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.	• Gestión de Incidentes	NO	L0
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información.	SI	Se debería utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro.	• Gestión de Incidentes	NO	L0
A.16.1.7	Recopilación de evidencias.	SI	La organización debería definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.	• Gestión de Incidentes	NO	L0
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.					
A.17.1	Continuidad de la seguridad de la información.					
A.17.1.1	Planificación de la continuidad de la seguridad de la información.	SI	La organización debería determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre.	• Gestión de la Continuidad del Negocio	(IND-019)	L0
A.17.1.2	Implantación de la continuidad de la seguridad de la información.	SI	La organización debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas.	• Gestión de la Continuidad del Negocio	(IND-019)	L0
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la Seguridad de la	SI	La organización debería verificar regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones	• Gestión de la Continuidad del Negocio	(IND-019)	L0

REF.	Control	Aplica SI/NO	Aplicabilidad	Procesos/Documentos	Indicador	Estado
	información.		adversas.			
A.17.2	Redundancias.					
A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	SI	Se debería implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.	• Gestión de la Continuidad del Negocio	NO	L1
A.18 A.18.1	CUMPLIMIENTO. Cumplimiento de los requisitos legales y contractuales.					
A.18.1.1	Identificación de la legislación aplicable.	SI	Se deberían identificar, documentar y mantener al día de manera explícita para cada sistema de información y para la organización todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la organización para cumplir con estos requisitos.	• Auditorías de Protección de datos	(IND-020)	L2
A.18.1.2	Derechos de propiedad intelectual (DPI).	SI	Se deberían implementar procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software originales.	• Inventario de Activos software	(IND-020)	L2
A.18.1.3	Protección de los registros de la organización.	SI	Los registros se deberían proteger contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.	• Gestión de Control de Accesos • Gestión de la Seguridad Física	(IND-020)	L2
A.18.1.4	Protección de datos y privacidad de la	SI	Se debería garantizar la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables	• Auditorías de Protección de datos	(IND-020)	L2

REF.	Control	Aplica SI/NO	Aplicabilidad	Procesos/Documentos	Indicador	Estado
	información personal.		que correspondan.			
A.18.1.5	Regulación de los controles criptográficos.	SI	Se deberían utilizar controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.	• Gestión de Operaciones y Comunicaciones	(IND-020)	L0
A.18.2	Revisiones de la seguridad de la información.					
A.18.2.1	Revisión independiente de la seguridad de la información.	SI	Se debería revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información en base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos en la organización.	• Procedimiento de Auditoría	NO	L1
A.18.2.2	Comprobación del cumplimiento	SI	Los gerentes deberían revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente.	• Actas Comisión Seguridad de la Información	NO	L1
A.18.2.3	Disponibilidad de instalaciones para el procesamiento de la información.	SI	Los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización.	• Procedimiento de Auditoría	NO	L1

16. Anexo IX. Amenazas por activo, Impacto Potencial y Riesgo Potencial

AUX	UPS	sistemas de alimentación ininterrumpida	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	B	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	100	B	MB
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	100	B	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	B	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	B	MB
I.4	DESASTRES INDUSTRIALES	Contaminación Electromagnética	1	PF	50	B	MB
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	1	PF	10	MB	MB
I.7	DESASTRES INDUSTRIALES	Condiciones inadecuadas de temperatura y/o humedad	1	PF	100	B	MB
I.10	DESASTRES INDUSTRIALES	Degradación de los soportes de almacenamiento de la información	1	PF	1	MB	MB
E.1	ERRORES	Errores de los usuarios	1	PF	100	B	MB
E.4	ERRORES	Errores de Configuración	1	PF	100	B	MB
E.7	ERRORES	Deficiencias en la organización	1	PF	100	B	MB
E.21	ERRORES	Errores de mantenimiento / actualización de programas (software)	1	PF	100	B	MB
E.23	ERRORES	Errores de mantenimiento / actualización de equipos (hardware)	1	PF	100	B	MB
E.24	ERRORES	Caida del sistema por agotamiento de recursos	1	PF	100	B	MB
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	B	MB
A.26	ATAQUES	Ataque Destructivo	1	PF	100	B	MB

AUX	GEN	generadores eléctricos	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	B	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	100	B	MB
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	100	B	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	B	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	B	MB
I.3	DESASTRES INDUSTRIALES	Contaminación Mecánica	1	PF	100	B	MB
I.4	DESASTRES INDUSTRIALES	Contaminación Electromagnética	1	PF	1	MB	MB
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	1	PF	100	B	MB
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	100	B	MB
E.1	ERRORES	Errores de los usuarios	1	PF	100	B	MB
E.2	ERRORES	Errores del administrador	1	PF	100	B	MB
E.3	ERRORES	Errores de monitorización (log)	1	PF	100	B	MB
E.4	ERRORES	Errores de Configuración	1	PF	100	B	MB
E.7	ERRORES	Deficiencias en la organización	1	PF	100	B	MB
E.23	ERRORES	Errores de mantenimiento / actualización de equipos (hardware)	1	PF	100	B	MB
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	B	MB
A.25	ATAQUES	Robo	1	PF	100	B	MB
A.26	ATAQUES	Ataque Destructivo	1	PF	100	B	MB
A.28	ATAQUES	Indisponibilidad del personal	2	FN	100	B	B

AUX	AC	equipos de climatización	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	B	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	100	B	MB
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	100	B	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	B	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	B	MB
I.3	DESASTRES INDUSTRIALES	Contaminación Mecánica	1	PF	1	MB	MB
I.4	DESASTRES INDUSTRIALES	Contaminación Electromagnética	1	PF	100	B	MB
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	100	B	B
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	100	B	MB
E.1	ERRORES	Errores de los usuarios	1	PF	10	MB	MB
E.2	ERRORES	Errores del administrador	1	PF	10	MB	MB
E.3	ERRORES	Errores de monitorización (log)	1	PF	10	MB	MB
E.4	ERRORES	Errores de Configuración	1	PF	10	MB	MB
E.7	ERRORES	Deficiencias en la organización	1	PF	10	MB	MB
E.23	ERRORES	Errores de mantenimiento / actualización de equipos (hardware)	2	FN	10	MB	MB
A.4	ATAQUES	Manipulación de la configuración	1	PF	10	MB	MB
A.25	ATAQUES	Robo	1	PF	10	MB	MB
A.26	ATAQUES	Ataque Destructivo	1	PF	100	B	MB
A.28	ATAQUES	Indisponibilidad del personal	2	FN	10	MB	MB

AUX	WIRE	cable eléctrico	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	B	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	100	B	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	B	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	B	MB
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	1	PF	100	B	MB
I.6	DESASTRES INDUSTRIALES	Corte de Suministro Electrico	2	FN	100	B	B
E.23	ERRORES	Errores de mantenimiento / actualización de equipos (hardware)	1	PF	100	B	MB
E.28	ERRORES	Indisponibilidad del personal	1	PF	10	MB	MB
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	B	MB
A.24	ATAQUES	Denegación de Servicio	1	PF	100	B	MB
A.25	ATAQUES	Robo	1	PF	100	B	MB
A.26	ATAQUES	Ataque Destructivo	1	PF	100	B	MB
A.28	ATAQUES	Indisponibilidad del personal	1	PF	10	MB	MB

AUX	FIBER	fibra óptica	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	B	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	B	MB
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	1	PF	100	B	MB
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	B	B
E.4	ERRORES	Errores de Configuración	1	PF	100	B	MB
E.23	ERRORES	Errores de mantenimiento / actualización de equipos (hardware)	1	PF	100	B	MB
E.28	ERRORES	Indisponibilidad del personal	1	PF	10	MB	MB
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	B	MB
A.26	ATAQUES	Ataque Destructivo	1	PF	100	B	MB
A.28	ATAQUES	Indisponibilidad del personal	1	PF	10	MB	MB

AUX	SUPPLY	suministros esenciales	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	B	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	100	B	MB
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	100	B	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	B	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	B	MB
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	100	B	B
I.9	DESASTRES INDUSTRIALES	Interrupción de otros servicios y suministros esenciales	2	FN	100	B	B
E.7	ERRORES	Deficiencias en la organización	2	FN	10	MB	MB
E.23	ERRORES	Errores de mantenimiento / actualización de equipos (hardware)	1	PF	10	MB	MB
A.26	ATAQUES	Ataque Destructivo	1	PF	10	MB	MB
A.28	ATAQUES	Indisponibilidad del personal	1	PF	10	MB	MB

AUX	FURNITURE	mobiliario: armarios, etc	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	B	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	100	B	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	B	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	B	MB
A.25	ATAQUES	Robo	2	FN	1	MB	MB
A.26	ATAQUES	Ataque Destructivo	1	PF	1	MB	MB

L	SITE	recinto	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	B	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	100	B	MB
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	100	B	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	B	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	B	MB
A.26	ATAQUES	Ataque Destructivo	1	PF	1	MB	MB

L	CAR	vehículo terrestre: ambulancias.	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	B	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	100	B	MB
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	100	B	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	B	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	B	MB
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	100	B	MB
E.23	ERRORES	Errores de mantenimiento / actualización de equipos (hardware)	2	FN	10	MB	MB
E.28	ERRORES	Indisponibilidad del personal	1	PF	100	B	MB
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	B	MB
A.25	ATAQUES	Robo	1	PF	100	B	MB
A.26	ATAQUES	Ataque Destructivo	1	PF	100	B	MB
A.28	ATAQUES	Indisponibilidad del personal	1	PF	100	B	MB

L	PLANE	vehículo aéreo: avión y helicoptero	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	B	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	100	B	MB
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	100	B	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	B	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	B	MB
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	100	B	MB
E.23	ERRORES	Errores de mantenimiento / actualización de equipos (hardware)	1	PF	100	B	MB
E.28	ERRORES	Indisponibilidad del personal	1	PF	100	B	MB
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	B	MB
A.25	ATAQUES	Robo	1	PF	100	B	MB
A.26	ATAQUES	Ataque Destructivo	1	PF	100	B	MB
A.28	ATAQUES	Indisponibilidad del personal	1	PF	100	B	MB

COM	PSTN	red telefónica	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	B	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	100	B	MB
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	100	B	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	B	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	B	MB
I.4	DESASTRES INDUSTRIALES	Contaminación Electromagnética	1	PF	100	B	MB
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	1	PF	100	B	MB
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	B	B
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	100	B	MB
E.4	ERRORES	Errores de Configuración	1	PF	10	MB	MB
E.21	ERRORES	Errores de mantenimiento / actualización de programas (software)	1	PF	10	MB	MB
E.23	ERRORES	Errores de mantenimiento / actualización de equipos (hardware)	1	PF	10	MB	MB
E.24	ERRORES	Caida del sistema por agotamiento de recursos	1	PF	100	B	MB
A.24	ATAQUES	Denegación de Servicio	1	PF	50	B	MB

COM	MAN	red metropolitana	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA	DEGRADACIÓN		IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	B	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	100	B	MB
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	100	B	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	B	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	B	MB
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	100	B	B
I.7	DESASTRES INDUSTRIALES	Condiciones inadecuadas de temperatura y/o humedad	1	PF	100	B	MB
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	B	B
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	100	B	MB
E.2	ERRORES	Errores del administrador	2	FN	50	B	B
E.3	ERRORES	Errores de monitorización (log)	1	PF	10	MB	MB
E.4	ERRORES	Errores de Configuración	2	FN	50	B	B
E.7	ERRORES	Deficiencias en la organización	1	PF	10	MB	MB
E.9	ERRORES	Errores de [re-]encamininamiento	1	PF	10	MB	MB
E.10	ERRORES	Errores de secuencia	1	PF	10	MB	MB
E.21	ERRORES	Errores de mantenimiento / actualización de programas (software)	2	FN	50	B	B
E.23	ERRORES	Errores de mantenimiento / actualización de equipos (hardware)	2	FN	50	B	B
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	B	MB
A.14	ATAQUES	Interceptación de información (escucha)	1	PF	1	MB	MB
A.15	ATAQUES	Modificación de la Información	1	PF	50	B	MB
A.16	ATAQUES	Introducción de información falsa	1	PF	50	B	MB
A.17	ATAQUES	Corrupción de la información	1	PF	100	B	MB
A.19	ATAQUES	Divulgación de la información	1	PF	1	MB	MB

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
A.24	ATAQUES	Denegación de Servicio	1	PF	50	B	MB
A.25	ATAQUES	Robo	1	PF	100	B	MB
A.26	ATAQUES	Ataque Destructivo	1	PF	100	B	MB

P	UI	usuarios internos	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	100	B	MB
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	100	B	MB
E.1	ERRORES	Errores de los usuarios	3	F	10	MB	B
E.7	ERRORES	Deficiencias en la organización	2	FN	10	MB	MB
E.8	ERRORES	Difusión de software dañino	2	FN	1	MB	MB
E.28	ERRORES	Indisponibilidad del personal	2	FN	10	MB	MB
A.5	ATAQUES	Suplantación de la identidad del usuario	4	MF	10	MB	M
A.28	ATAQUES	Indisponibilidad del personal	1	PF	10	MB	MB
A.29	ATAQUES	Extorsion	1	PF	10	MB	MB
A.30	ATAQUES	Ingenieria social	3	F	10	MB	B

P	OP	operadores	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	10	MB	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	10	MB	MB
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	10	MB	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	10	MB	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	10	MB	MB
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	10	MB	MB
E.1	ERRORES	Errores de los usuarios	3	F	1	MB	B
E.2	ERRORES	Errores del administrador	2	FN	50	B	B
E.3	ERRORES	Errores de monitorización (log)	2	FN	50	B	B
E.4	ERRORES	Errores de Configuración	2	FN	50	B	B
E.7	ERRORES	Deficiencias en la organización	2	FN	50	B	B
E.28	ERRORES	Indisponibilidad del personal	1	PF	10	MB	MB
A.28	ATAQUES	Indisponibilidad del personal	1	PF	10	MB	MB
A.29	ATAQUES	Extorsion	1	PF	10	MB	MB
A.30	ATAQUES	Ingenieria social	1	PF	10	MB	MB

P	ADM	administradores de sistemas	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	50	B	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	50	B	MB
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	50	B	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	50	B	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	50	B	MB
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	50	B	MB
E.2	ERRORES	Errores del administrador	2	FN	10	MB	MB
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	MB	MB
E.4	ERRORES	Errores de Configuración	2	FN	10	MB	MB
E.7	ERRORES	Deficiencias en la organización	1	PF	10	MB	MB
E.28	ERRORES	Indisponibilidad del personal	1	PF	10	MB	MB
A.28	ATAQUES	Indisponibilidad del personal	1	PF	10	MB	MB
A.29	ATAQUES	Extorsion	1	PF	10	MB	MB
A.30	ATAQUES	Ingenieria social	1	PF	10	MB	MB

P	COM	administradores de comunicaciones	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	50	B	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	50	B	MB
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	50	B	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	50	B	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	50	B	MB
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	50	B	MB
E.2	ERRORES	Errores del administrador	2	FN	10	MB	MB
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	MB	MB
E.4	ERRORES	Errores de Configuración	2	FN	10	MB	MB
E.7	ERRORES	Deficiencias en la organización	1	PF	10	MB	MB
E.28	ERRORES	Indisponibilidad del personal	1	PF	10	MB	MB
A.28	ATAQUES	Indisponibilidad del personal	1	PF	10	MB	MB
A.29	ATAQUES	Extorsion	1	PF	10	MB	MB
A.30	ATAQUES	Ingenieria social	1	PF	10	MB	MB

P	DBA	administradores de BBDD	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	50	B	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	50	B	MB
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	50	B	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	50	B	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	50	B	MB
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	50	B	MB
E.2	ERRORES	Errores del administrador	2	FN	10	MB	MB
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	MB	MB
E.4	ERRORES	Errores de Configuración	2	FN	10	MB	MB
E.7	ERRORES	Deficiencias en la organización	1	PF	10	MB	MB
E.28	ERRORES	Indisponibilidad del personal	1	PF	10	MB	MB
A.28	ATAQUES	Indisponibilidad del personal	1	PF	10	MB	MB
A.29	ATAQUES	Extorsion	1	PF	10	MB	MB
A.30	ATAQUES	Ingenieria social	1	PF	10	MB	MB

P	SUB	subcontratas	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	10	MB	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	10	MB	MB
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	10	MB	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	10	MB	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	10	MB	MB
E.2	ERRORES	Errores del administrador	2	FN	10	MB	MB
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	MB	MB
E.4	ERRORES	Errores de Configuración	2	FN	10	MB	MB
E.7	ERRORES	Deficiencias en la organización	2	FN	10	MB	MB
E.28	ERRORES	Indisponibilidad del personal	1	PF	10	MB	MB
A.28	ATAQUES	Indisponibilidad del personal	1	PF	10	MB	MB
A.29	ATAQUES	Extorsion	1	PF	10	MB	MB
A.30	ATAQUES	Ingenieria social	1	PF	10	MB	MB

HW	MID	equipos medios	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	B	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	100	B	MB
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	100	B	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	B	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	B	MB
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	10	MB	MB
I.6	DESASTRES INDUSTRIALES	Corte de Suministro Electrico	1	PF	100	B	MB
I.7	DESASTRES INDUSTRIALES	Condiciones inadecuadas de temperatura y/o humedad	1	PF	100	B	MB
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	B	B
I.10	DESASTRES INDUSTRIALES	Degradación de los soportes de almacenamiento de la información	1	PF	100	B	MB
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	100	B	MB
E.1	ERRORES	Errores de los usuarios	1	PF	10	MB	MB
E.2	ERRORES	Errores del administrador	2	FN	10	MB	MB
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	MB	MB
E.4	ERRORES	Errores de Configuración	2	FN	10	MB	MB
E.8	ERRORES	Difusión de software dañino	1	PF	10	MB	MB
E.23	ERRORES	Errores de mantenimiento / actualización de equipos (hardware)	2	FN	10	MB	MB
E.24	ERRORES	Caida del sistema por agotamiento de recursos	1	PF	100	B	MB
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	B	MB
A.25	ATAQUES	Robo	1	PF	100	B	MB
A.26	ATAQUES	Ataque Destructivo	1	PF	100	B	MB

HW	PC	informática personal	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	1	MB	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	1	MB	MB
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	1	MB	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	1	MB	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	1	MB	MB
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	1	MB	MB
I.6	DESASTRES INDUSTRIALES	Corte de Suministro Electrico	1	PF	10	MB	MB
I.7	DESASTRES INDUSTRIALES	Condiciones inadecuadas de temperatura y/o humedad	1	PF	1	MB	MB
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	B	B
I.10	DESASTRES INDUSTRIALES	Degradación de los soportes de almacenamiento de la información	1	PF	1	MB	MB
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	1	MB	MB
E.1	ERRORES	Errores de los usuarios	2	FN	100	B	B
E.2	ERRORES	Errores del administrador	2	FN	100	B	B
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	MB	MB
E.4	ERRORES	Errores de Configuración	2	FN	100	B	B
E.7	ERRORES	Deficiencias en la organización	2	FN	10	MB	MB
E.23	ERRORES	Errores de mantenimiento / actualización de equipos (hardware)	2	FN	100	B	B
E.24	ERRORES	Caida del sistema por agotamiento de recursos	1	PF	1	MB	MB
E.28	ERRORES	Indisponibilidad del personal	1	PF	1	MB	MB
A.4	ATAQUES	Manipulación de la configuración	1	PF	1	MB	MB
A.25	ATAQUES	Robo	2	FN	1	MB	MB
A.26	ATAQUES	Ataque Destructivo	1	PF	1	MB	MB
A.28	ATAQUES	Indisponibilidad del personal	1	PF	1	MB	MB

HW	PC	informática personal	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA	DEGRADACIÓN		IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	B	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	100	B	MB
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	100	B	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	B	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	B	MB
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	100	B	B
I.6	DESASTRES INDUSTRIALES	Corte de Suministro Electrico	1	PF	100	B	MB
I.7	DESASTRES INDUSTRIALES	Condiciones inadecuadas de temperatura y/o humedad	1	PF	100	B	MB
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	B	B
I.10	DESASTRES INDUSTRIALES	Degradación de los soportes de almacenamiento de la información	1	PF	100	B	MB
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	100	B	MB
E.1	ERRORES	Errores de los usuarios	1	PF	1	MB	MB
E.2	ERRORES	Errores del administrador	2	FN	100	B	B
E.3	ERRORES	Errores de monitorización (log)	2	FN	1	MB	MB
E.4	ERRORES	Errores de Configuración	2	FN	100	B	B
E.7	ERRORES	Deficiencias en la organización	2	FN	10	MB	MB
E.23	ERRORES	Errores de mantenimiento / actualización de equipos (hardware)	2	FN	100	B	B
E.24	ERRORES	Caida del sistema por agotamiento de recursos	1	PF	100	B	MB
E.28	ERRORES	Indisponibilidad del personal	2	FN	1	MB	MB
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	B	MB
A.25	ATAQUES	Robo	1	PF	100	B	MB

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
A.26	ATAQUES	Ataque Destructivo	1	PF	100	B	MB
A.28	ATAQUES	Indisponibilidad del personal	1	PF	1	MB	MB

HW	PRINT	medios de impresión	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	1	MB	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	1	MB	MB
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	1	MB	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	1	MB	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	1	MB	MB
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	1	MB	MB
I.6	DESASTRES INDUSTRIALES	Corte de Suministro Electrico	1	PF	1	MB	MB
I.7	DESASTRES INDUSTRIALES	Condiciones inadecuadas de temperatura y/o humedad	1	PF	1	MB	MB
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	B	B
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	1	MB	MB
E.1	ERRORES	Errores de los usuarios	2	FN	1	MB	MB
E.2	ERRORES	Errores del administrador	2	FN	1	MB	MB
E.3	ERRORES	Errores de monitorización (log)	2	FN	1	MB	MB
E.4	ERRORES	Errores de Configuración	2	FN	1	MB	MB
E.7	ERRORES	Deficiencias en la organización	2	FN	1	MB	MB
E.23	ERRORES	Errores de mantenimiento / actualización de equipos (hardware)	2	FN	1	MB	MB
E.28	ERRORES	Indisponibilidad del personal	1	PF	1	MB	MB

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
A.4	ATAQUES	Manipulación de la configuración	1	PF	1	MB	MB
A.25	ATAQUES	Robo	2	FN	1	MB	MB
A.26	ATAQUES	Ataque Destructivo	1	PF	1	MB	MB
A.28	ATAQUES	Indisponibilidad del personal	1	PF	1	MB	MB

HW	SWITCH	conmutadores	M

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	M	B
N.2	DESASTRES NATURALES	Daños por agua	1	PF	100	M	B
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	100	M	B
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	M	B
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	M	B
I.4	DESASTRES INDUSTRIALES	Contaminación Electromagnética	1	PF	100	M	B
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	100	M	M
I.6	DESASTRES INDUSTRIALES	Corte de Suministro Electrico	2	FN	100	M	M
I.7	DESASTRES INDUSTRIALES	Condiciones inadecuadas de temperatura y/o humedad	1	PF	100	M	B
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	M	M
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	100	M	B
E.2	ERRORES	Errores del administrador	2	FN	100	M	M
E.3	ERRORES	Errores de monitorización (log)	2	FN	100	M	M
E.4	ERRORES	Errores de Configuración	2	FN	100	M	M
E.7	ERRORES	Deficiencias en la organización	1	PF	10	B	MB

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.9	ERRORES	Errores de [re-]encamininamiento	1	PF	100	M	B
E.10	ERRORES	Errores de secuencia	1	PF	100	M	B
E.28	ERRORES	Indisponibilidad del personal	1	PF	10	B	MB
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	M	B
A.25	ATAQUES	Robo	1	PF	100	M	B
A.26	ATAQUES	Ataque Destructivo	1	PF	100	M	B
A.28	ATAQUES	Indisponibilidad del personal	1	PF	10	B	MB

HW	BRIDGE	pasarelas	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	B	MB
N.2	DESASTRES NATURALES	Daños por agua	1	PF	100	B	MB
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	100	B	MB
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	B	MB
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	B	MB
I.4	DESASTRES INDUSTRIALES	Contaminación Electromagnética	1	PF	100	B	MB
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	100	B	B
I.6	DESASTRES INDUSTRIALES	Corte de Suministro Electrico	1	PF	100	B	MB
I.7	DESASTRES INDUSTRIALES	Condiciones inadecuadas de temperatura y/o humedad	1	PF	100	B	MB
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	B	B
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	100	B	MB
E.2	ERRORES	Errores del administrador	2	FN	100	B	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.3	ERRORES	Errores de monitorización (log)	2	FN	100	B	B
E.4	ERRORES	Errores de Configuración	2	FN	100	B	B
E.7	ERRORES	Deficiencias en la organización	1	PF	10	MB	MB
E.9	ERRORES	Errores de [re-]encamininamiento	1	PF	100	B	MB
E.10	ERRORES	Errores de secuencia	1	PF	100	B	MB
E.28	ERRORES	Indisponibilidad del personal	1	PF	100	B	MB
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	B	MB
A.25	ATAQUES	Robo	1	PF	100	B	MB
A.26	ATAQUES	Ataque Destructivo	1	PF	100	B	MB
A.28	ATAQUES	Indisponibilidad del personal	1	PF	100	B	MB

HW FIREWALL cortafuegos A

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	A	M
N.2	DESASTRES NATURALES	Daños por agua	1	PF	100	A	M
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	100	A	M
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	A	M
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	A	M
I.4	DESASTRES INDUSTRIALES	Contaminación Electromagnética	1	PF	100	A	M
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	100	A	A
I.6	DESASTRES INDUSTRIALES	Corte de Suministro Electrico	1	PF	100	A	M
I.7	DESASTRES INDUSTRIALES	Condiciones inadecuadas de temperatura y/o humedad	1	PF	100	A	M

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	A	A
I.10	DESASTRES INDUSTRIALES	Degradación de los soportes de almacenamiento de la información	1	PF	100	A	M
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	100	A	M
E.2	ERRORES	Errores del administrador	2	FN	100	A	A
E.3	ERRORES	Errores de monitorización (log)	2	FN	100	A	A
E.4	ERRORES	Errores de Configuración	2	FN	100	A	A
E.7	ERRORES	Deficiencias en la organización	1	PF	10	M	B
E.23	ERRORES	Errores de mantenimiento / actualización de equipos (hardware)	2	FN	100	A	A
E.24	ERRORES	Caida del sistema por agotamiento de recursos	1	PF	100	A	M
E.28	ERRORES	Indisponibilidad del personal	1	PF	10	M	B
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	A	M
A.25	ATAQUES	Robo	1	PF	100	A	M
A.26	ATAQUES	Ataque Destructivo	4	MF	100	A	**MA**
A.28	ATAQUES	Indisponibilidad del personal	1	PF	100	A	M

MEDIA	**SAN**	**almacenamiento en red**	**MA**

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	MA	A
N.2	DESASTRES NATURALES	Daños por agua	1	PF	100	MA	A
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	100	MA	A
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	MA	A
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	MA	A

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
I.4	DESASTRES INDUSTRIALES	Contaminación Electromagnética	1	PF	100	MA	A
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	1	PF	100	MA	A
I.6	DESASTRES INDUSTRIALES	Corte de Suministro Electrico	1	PF	100	MA	A
I.7	DESASTRES INDUSTRIALES	Condiciones inadecuadas de temperatura y/o humedad	1	PF	100	MA	A
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	MA	**MA**
I.10	DESASTRES INDUSTRIALES	Degradación de los soportes de almacenamiento de la información	1	PF	100	MA	A
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	100	MA	A
E.2	ERRORES	Errores del administrador	2	FN	100	MA	**MA**
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	A	A
E.4	ERRORES	Errores de Configuración	2	FN	100	MA	**MA**
E.7	ERRORES	Deficiencias en la organización	1	PF	10	A	M
E.28	ERRORES	Indisponibilidad del personal	1	PF	10	A	M
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	MA	A
A.25	ATAQUES	Robo	1	PF	100	MA	A
A.26	ATAQUES	Ataque Destructivo	1	PF	100	MA	A
A.28	ATAQUES	Indisponibilidad del personal	1	PF	100	MA	A

S DIR servicio de directorio B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	100	B	B
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	B	B
I.9	DESASTRES INDUSTRIALES	Interrupción de otros servicios y suministros esenciales	1	PF	1	MB	MB

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
I.10	DESASTRES INDUSTRIALES	Degradación de los soportes de almacenamiento de la información	1	PF	100	B	MB
E.2	ERRORES	Errores del administrador	2	FN	100	B	B
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	MB	MB
E.4	ERRORES	Errores de Configuración	2	FN	100	B	B
E.7	ERRORES	Deficiencias en la organización	2	FN	10	MB	MB
E.8	ERRORES	Difusión de software dañino	4	MF	10	MB	M
E.16	ERRORES	Introducción de información incorrecta	2	FN	10	MB	MB
E.17	ERRORES	Degradación de la Información	1	PF	10	MB	MB
E.18	ERRORES	Destrucción de la información	1	PF	100	B	MB
E.19	ERRORES	Divulgación de la información	1	PF	1	MB	MB
E.20	ERRORES	Vulnerabilidades de los programas (software)	1	PF	10	MB	MB
E.21	ERRORES	Errores de mantenimiento / actualización de programas (software)	2	FN	100	B	B
E.24	ERRORES	Caida del sistema por agotamiento de recursos	2	FN	100	B	B
E.28	ERRORES	Indisponibilidad del personal	1	PF	10	MB	MB
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	B	MB
A.5	ATAQUES	Suplantación de la identidad del usuario	1	PF	10	MB	MB
A.6	ATAQUES	Abuso de privilegios de acceso	1	PF	10	MB	MB
A.8	ATAQUES	Difusión de software dañino	4	MF	10	MB	M
A.15	ATAQUES	Modificación de la Información	1	PF	10	MB	MB
A.16	ATAQUES	Introducción de información falsa	1	PF	10	MB	MB
A.17	ATAQUES	Corrupción de la información	1	PF	10	MB	MB
A.18	ATAQUES	Destrucción de la información	1	PF	100	B	MB
A.19	ATAQUES	Divulgación de la información	1	PF	1	MB	MB
A.22	ATAQUES	Manipulación de los programas	1	PF	1	MB	MB
A.24	ATAQUES	Denegación de Servicio	1	PF	50	B	MB

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA	DEGRADACIÓN		IMPACTO POTENCIAL	RIESGO POTENCIAL
A.28	ATAQUES	Indisponibilidad del personal	1	PF	1	MB	MB

S	**IDM**	**gestión de identidades**	**B**

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA	DEGRADACIÓN		IMPACTO POTENCIAL	RIESGO POTENCIAL
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	1	PF	100	B	MB
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	B	B
I.9	DESASTRES INDUSTRIALES	Interrupción de otros servicios y suministros esenciales	1	PF	100	B	MB
I.10	DESASTRES INDUSTRIALES	Degradación de los soportes de almacenamiento de la información	1	PF	100	B	MB
E.2	ERRORES	Errores del administrador	2	FN	100	B	B
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	MB	MB
E.4	ERRORES	Errores de Configuración	2	FN	100	B	B
E.7	ERRORES	Deficiencias en la organización	2	FN	10	MB	MB
E.8	ERRORES	Difusión de software dañino	4	MF	10	MB	M
E.16	ERRORES	Introducción de información incorrecta	2	FN	10	MB	MB
E.17	ERRORES	Degradación de la Información	1	PF	10	MB	MB
E.18	ERRORES	Destrucción de la información	1	PF	100	B	MB
E.19	ERRORES	Divulgación de la información	1	PF	1	MB	MB
E.20	ERRORES	Vulnerabilidades de los programas (software)	2	FN	10	MB	MB
E.21	ERRORES	Errores de mantenimiento / actualización de programas (software)	2	FN	100	B	B
E.24	ERRORES	Caida del sistema por agotamiento de recursos	2	FN	100	B	B
E.28	ERRORES	Indisponibilidad del personal	1	PF	10	MB	MB
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	B	MB

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
A.5	ATAQUES	Suplantación de la identidad del usuario	1	PF	1	MB	MB
A.6	ATAQUES	Abuso de privilegios de acceso	1	PF	100	B	MB
A.8	ATAQUES	Difusión de software dañino	3	F	10	MB	B
A.15	ATAQUES	Modificación de la Información	1	PF	10	MB	MB
A.16	ATAQUES	Introducción de información falsa	1	PF	10	MB	MB
A.17	ATAQUES	Corrupción de la información	1	PF	10	MB	MB
A.18	ATAQUES	Destrucción de la información	1	PF	100	B	MB
A.19	ATAQUES	Divulgación de la información	1	PF	1	MB	MB
A.22	ATAQUES	Manipulación de los programas	1	PF	10	MB	MB
A.24	ATAQUES	Denegación de Servicio	1	PF	100	B	MB
A.28	ATAQUES	Indisponibilidad del personal	1	PF	10	MB	MB

S	**IPM**	**gestión de privilegios**	**B**

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	100	B	B
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	B	B
I.9	DESASTRES INDUSTRIALES	Interrupción de otros servicios y suministros esenciales	1	PF	100	B	MB
I.10	DESASTRES INDUSTRIALES	Degradación de los soportes de almacenamiento de la información	1	PF	100	B	MB
E.2	ERRORES	Errores del administrador	2	FN	100	B	B
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	MB	MB
E.4	ERRORES	Errores de Configuración	2	FN	100	B	B
E.7	ERRORES	Deficiencias en la organización	2	FN	10	MB	MB

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.8	ERRORES	Difusión de software dañino	4	MF	10	MB	M
E.16	ERRORES	Introducción de información incorrecta	2	FN	10	MB	MB
E.17	ERRORES	Degradación de la Información	1	PF	10	MB	MB
E.18	ERRORES	Destrucción de la información	1	PF	100	B	MB
E.19	ERRORES	Divulgación de la información	1	PF	1	MB	MB
E.20	ERRORES	Vulnerabilidades de los programas (software)	2	FN	10	MB	MB
E.21	ERRORES	Errores de mantenimiento / actualización de programas (software)	2	FN	100	B	B
E.24	ERRORES	Caida del sistema por agotamiento de recursos	1	PF	100	B	MB
E.28	ERRORES	Indisponibilidad del personal	1	PF	10	MB	MB
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	B	MB
A.5	ATAQUES	Suplantación de la identidad del usuario	1	PF	1	MB	MB
A.6	ATAQUES	Abuso de privilegios de acceso	1	PF	100	B	MB
A.8	ATAQUES	Difusión de software dañino	1	PF	10	MB	MB
A.15	ATAQUES	Modificación de la Información	1	PF	10	MB	MB
A.16	ATAQUES	Introducción de información falsa	1	PF	10	MB	MB
A.17	ATAQUES	Corrupción de la información	1	PF	10	MB	MB
A.18	ATAQUES	Destrucción de la información	1	PF	100	B	MB
A.19	ATAQUES	Divulgación de la información	1	PF	1	MB	MB
A.22	ATAQUES	Manipulación de los programas	1	PF	10	MB	MB
A.24	ATAQUES	Denegación de Servicio	1	PF	100	B	MB
A.28	ATAQUES	Indisponibilidad del personal	1	PF	10	MB	MB

SW	BROWSER	navegador web	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA	DEGRADACIÓN		IMPACTO POTENCIAL	RIESGO POTENCIAL
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	1	PF	100	B	MB
E.1	ERRORES	Errores de los usuarios	3	F	100	B	M
E.2	ERRORES	Errores del administrador	2	FN	100	B	B
E.4	ERRORES	Errores de Configuración	2	FN	100	B	B
E.8	ERRORES	Difusión de software dañino	4	MF	10	MB	M
E.20	ERRORES	Vulnerabilidades de los programas (software)	2	FN	10	MB	MB
E.21	ERRORES	Errores de mantenimiento / actualización de programas (software)	2	FN	100	B	B
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	B	MB
A.7	ATAQUES	Uso no previsto	4	MF	10	MB	M
A.8	ATAQUES	Difusión de software dañino	4	MF	10	MB	M
A.22	ATAQUES	Manipulación de los programas	1	PF	10	MB	MB
A.28	ATAQUES	Indisponibilidad del personal	1	PF	10	MB	MB

SW	WWW	servidor de presentación	A

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA	DEGRADACIÓN		IMPACTO POTENCIAL	RIESGO POTENCIAL
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	100	A	A
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	A	A
E.2	ERRORES	Errores del administrador	2	FN	100	A	A
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	M	M
E.4	ERRORES	Errores de Configuración	2	FN	100	A	A

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.8	ERRORES	Difusión de software dañino	4	MF	10	M	MA
E.20	ERRORES	Vulnerabilidades de los programas (software)	2	FN	10	M	M
E.21	ERRORES	Errores de mantenimiento / actualización de programas (software)	2	FN	100	A	A
E.24	ERRORES	Caida del sistema por agotamiento de recursos	1	PF	100	A	M
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	A	M
A.14	ATAQUES	Interceptación de información (escucha)	1	PF	1	M	B
A.15	ATAQUES	Modificación de la Información	1	PF	10	M	B
A.16	ATAQUES	Introducción de información falsa	1	PF	10	M	B
A.17	ATAQUES	Corrupción de la información	1	PF	10	M	B
A.18	ATAQUES	Destrucción de la información	1	PF	100	A	M
A.19	ATAQUES	Divulgación de la información	1	PF	1	M	B
A.22	ATAQUES	Manipulación de los programas	1	PF	10	M	B
A.24	ATAQUES	Denegación de Servicio	1	PF	100	A	M

SW	APP	servidor de aplicaciones	A

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	100	A	A
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	A	A
E.2	ERRORES	Errores del administrador	2	FN	100	A	A
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	M	M
E.4	ERRORES	Errores de Configuración	2	FN	100	A	A
E.8	ERRORES	Difusión de software dañino	4	MF	10	M	MA

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.20	ERRORES	Vulnerabilidades de los programas (software)	2	FN	10	M	M
E.21	ERRORES	Errores de mantenimiento / actualización de programas (software)	2	FN	100	A	A
E.24	ERRORES	Caida del sistema por agotamiento de recursos	1	PF	100	A	M
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	A	M
A.14	ATAQUES	Interceptación de información (escucha)	1	PF	1	M	B
A.15	ATAQUES	Modificación de la Información	1	PF	10	M	B
A.16	ATAQUES	Introducción de información falsa	1	PF	10	M	B
A.17	ATAQUES	Corrupción de la información	1	PF	10	M	B
A.18	ATAQUES	Destrucción de la información	1	PF	100	A	M
A.19	ATAQUES	Divulgación de la información	1	PF	1	M	B
A.22	ATAQUES	Manipulación de los programas	1	PF	10	M	B
A.24	ATAQUES	Denegación de Servicio	1	PF	100	A	M

SW	DBMS	sistema de gestión de bases de datos	A

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	100	A	A
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	A	A
E.2	ERRORES	Errores del administrador	2	FN	100	A	A
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	M	M
E.4	ERRORES	Errores de Configuración	2	FN	100	A	A
E.8	ERRORES	Difusión de software dañino	4	MF	10	M	MA
E.20	ERRORES	Vulnerabilidades de los programas (software)	2	FN	10	M	M

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA	DEGRADACIÓN		IMPACTO POTENCIAL	RIESGO POTENCIAL
E.21	ERRORES	Errores de mantenimiento / actualización de programas (software)	2	FN	100	A	A
E.24	ERRORES	Caida del sistema por agotamiento de recursos	1	PF	100	A	M
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	A	M
A.5	ATAQUES	Suplantación de la identidad del usuario	1	PF	1	M	B
A.6	ATAQUES	Abuso de privilegios de acceso	1	PF	100	A	M
A.11	ATAQUES	Acceso no autorizado	1	PF	100	A	M
A.14	ATAQUES	Interceptación de información (escucha)	1	PF	1	M	B
A.15	ATAQUES	Modificación de la Información	1	PF	100	A	M
A.16	ATAQUES	Introducción de información falsa	1	PF	100	A	M
A.17	ATAQUES	Corrupción de la información	1	PF	100	A	M
A.18	ATAQUES	Destrucción de la información	1	PF	100	A	M
A.19	ATAQUES	Divulgación de la información	1	PF	1	M	B
A.22	ATAQUES	Manipulación de los programas	1	PF	10	M	B
A.24	ATAQUES	Denegación de Servicio	1	PF	100	A	M

SW	**AV**	**anti virus**	**B**

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA	DEGRADACIÓN		IMPACTO POTENCIAL	RIESGO POTENCIAL
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	100	B	B
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	B	B
E.2	ERRORES	Errores del administrador	2	FN	100	B	B
E.3	ERRORES	Errores de monitorización (log)	2	FN	100	B	B
E.4	ERRORES	Errores de Configuración	2	FN	100	B	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.8	ERRORES	Difusión de software dañino	3	F	100	B	M
E.20	ERRORES	Vulnerabilidades de los programas (software)	2	FN	100	B	B
E.21	ERRORES	Errores de mantenimiento / actualización de programas (software)	2	FN	100	B	B
E.24	ERRORES	Caida del sistema por agotamiento de recursos	1	PF	100	B	MB
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	B	MB
A.14	ATAQUES	Interceptación de información (escucha)	1	PF	1	MB	MB
A.15	ATAQUES	Modificación de la Información	1	PF	10	MB	MB
A.16	ATAQUES	Introducción de información falsa	1	PF	10	MB	MB
A.17	ATAQUES	Corrupción de la información	1	PF	10	MB	MB
A.18	ATAQUES	Destrucción de la información	1	PF	10	MB	MB
A.19	ATAQUES	Divulgación de la información	1	PF	1	MB	MB
A.22	ATAQUES	Manipulación de los programas	1	PF	10	MB	MB
A.24	ATAQUES	Denegación de Servicio	1	PF	100	B	MB

SW	OS	sistema operativo	A

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	100	A	A
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	A	A
E.2	ERRORES	Errores del administrador	2	FN	100	A	A
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	M	M
E.4	ERRORES	Errores de Configuración	2	FN	100	A	A
E.8	ERRORES	Difusión de software dañino	4	MF	10	M	MA

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.20	ERRORES	Vulnerabilidades de los programas (software)	2	FN	10	M	M
E.21	ERRORES	Errores de mantenimiento / actualización de programas (software)	2	FN	100	A	A
E.24	ERRORES	Caida del sistema por agotamiento de recursos	2	FN	100	A	A
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	A	M
A.5	ATAQUES	Suplantación de la identidad del usuario	1	PF	10	M	B
A.6	ATAQUES	Abuso de privilegios de acceso	1	PF	100	A	M
A.11	ATAQUES	Acceso no autorizado	1	PF	10	M	B
A.14	ATAQUES	Interceptación de información (escucha)	1	PF	1	M	B
A.15	ATAQUES	Modificación de la Información	1	PF	10	M	B
A.16	ATAQUES	Introducción de información falsa	1	PF	10	M	B
A.17	ATAQUES	Corrupción de la información	1	PF	10	M	B
A.18	ATAQUES	Destrucción de la información	1	PF	100	A	M
A.19	ATAQUES	Divulgación de la información	1	PF	1	M	B
A.22	ATAQUES	Manipulación de los programas	1	PF	10	M	B
A.24	ATAQUES	Denegación de Servicio	1	PF	100	A	M

SW HYPERVISOR gestor de máquinas virtuales A

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	100	A	A
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	A	A
E.2	ERRORES	Errores del administrador	2	FN	100	A	A
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	M	M

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.4	ERRORES	Errores de Configuración	2	FN	100	A	A
E.8	ERRORES	Difusión de software dañino	4	MF	10	M	MA
E.20	ERRORES	Vulnerabilidades de los programas (software)	2	FN	10	M	M
E.21	ERRORES	Errores de mantenimiento / actualización de programas (software)	2	FN	100	A	A
E.24	ERRORES	Caida del sistema por agotamiento de recursos	1	PF	100	A	M
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	A	M
A.14	ATAQUES	Interceptación de información (escucha)	1	PF	10	M	B
A.15	ATAQUES	Modificación de la Información	1	PF	100	A	M
A.16	ATAQUES	Introducción de información falsa	1	PF	100	A	M
A.17	ATAQUES	Corrupción de la información	1	PF	100	A	M
A.18	ATAQUES	Destrucción de la información	1	PF	100	A	M
A.19	ATAQUES	Divulgación de la información	1	PF	10	M	B
A.22	ATAQUES	Manipulación de los programas	1	PF	10	M	B
A.24	ATAQUES	Denegación de Servicio	1	PF	100	A	M

SW	TS	servidor de terminales	A

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	100	A	A
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	A	A
E.2	ERRORES	Errores del administrador	2	FN	100	A	A
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	M	M
E.4	ERRORES	Errores de Configuración	2	FN	100	A	A

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.8	ERRORES	Difusión de software dañino	4	MF	10	M	MA
E.20	ERRORES	Vulnerabilidades de los programas (software)	2	FN	10	M	M
E.21	ERRORES	Errores de mantenimiento / actualización de programas (software)	2	FN	100	A	A
E.24	ERRORES	Caida del sistema por agotamiento de recursos	1	PF	100	A	M
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	A	M
A.14	ATAQUES	Interceptación de información (escucha)	1	PF	1	M	B
A.15	ATAQUES	Modificación de la Información	1	PF	100	A	M
A.16	ATAQUES	Introducción de información falsa	1	PF	100	A	M
A.17	ATAQUES	Corrupción de la información	1	PF	100	A	M
A.18	ATAQUES	Destrucción de la información	1	PF	100	A	M
A.19	ATAQUES	Divulgación de la información	1	PF	1	M	B
A.22	ATAQUES	Manipulación de los programas	1	PF	10	M	B
A.24	ATAQUES	Denegación de Servicio	1	PF	100	A	M

SW	BACKUP	sistema de backup	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	100	B	B
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	B	B
E.2	ERRORES	Errores del administrador	2	FN	100	B	B
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	MB	MB
E.4	ERRORES	Errores de Configuración	2	FN	100	B	B
E.8	ERRORES	Difusión de software dañino	4	MF	10	MB	M

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.20	ERRORES	Vulnerabilidades de los programas (software)	2	FN	10	MB	MB
E.21	ERRORES	Errores de mantenimiento / actualización de programas (software)	2	FN	100	B	B
E.24	ERRORES	Caida del sistema por agotamiento de recursos	1	PF	100	B	MB
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	B	MB
A.14	ATAQUES	Interceptación de información (escucha)	1	PF	1	MB	MB
A.15	ATAQUES	Modificación de la Información	1	PF	100	B	MB
A.16	ATAQUES	Introducción de información falsa	1	PF	100	B	MB
A.17	ATAQUES	Corrupción de la información	1	PF	100	B	MB
A.18	ATAQUES	Destrucción de la información	1	PF	100	B	MB
A.19	ATAQUES	Divulgación de la información	1	PF	1	MB	MB
A.22	ATAQUES	Manipulación de los programas	1	PF	10	MB	MB
A.24	ATAQUES	Denegación de Servicio	1	PF	100	B	MB

D PERA Datos de carácter personal nivel alto A

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.1	ERRORES	Errores de los usuarios	4	MF	100	A	MA
E.2	ERRORES	Errores del administrador	2	FN	100	A	A
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	M	M
E.4	ERRORES	Errores de Configuración	2	FN	10	M	M
E.7	ERRORES	Deficiencias en la organización	2	FN	50	A	A
E.15	ERRORES	Alteración de la información	4	MF	100	A	MA
E.16	ERRORES	Introducción de información incorrecta	4	MF	100	A	MA

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.17	ERRORES	Degradación de la Información	1	PF	100	A	M
E.18	ERRORES	Destrucción de la información	1	PF	100	A	M
E.19	ERRORES	Divulgación de la información	4	MF	10	M	MA
A.5	ATAQUES	Suplantación de la identidad del usuario	4	MF	1	M	MA
A.6	ATAQUES	Abuso de privilegios de acceso	1	PF	100	A	M
A.7	ATAQUES	Uso no previsto	3	F	10	M	A
A.15	ATAQUES	Modificación de la Información	1	PF	100	A	M
A.16	ATAQUES	Introducción de información falsa	1	PF	100	A	M
A.17	ATAQUES	Corrupción de la información	1	PF	100	A	M
A.18	ATAQUES	Destrucción de la información	1	PF	100	A	M
A.19	ATAQUES	Divulgación de la información	1	PF	10	M	B

D BACKUP Copias de respaldo M

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	M	B
N.2	DESASTRES NATURALES	Daños por agua	1	PF	100	M	B
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	100	M	B
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	M	B
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	M	B
I.4	DESASTRES INDUSTRIALES	Contaminación Electromagnética	1	PF	100	M	B
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	1	PF	100	M	B
I.7	DESASTRES INDUSTRIALES	Condiciones inadecuadas de temperatura y/o humedad	1	PF	100	M	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
I.10	DESASTRES INDUSTRIALES	Degradación de los soportes de almacenamiento de la información	1	PF	100	M	B
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	100	M	B
E.2	ERRORES	Errores del administrador	2	FN	100	M	M
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	B	B
E.4	ERRORES	Errores de Configuración	2	FN	100	M	M
E.7	ERRORES	Deficiencias en la organización	2	FN	100	M	M
E.16	ERRORES	Introducción de información incorrecta	1	PF	100	M	B
E.17	ERRORES	Degradación de la Información	1	PF	100	M	B
E.18	ERRORES	Destrucción de la información	1	PF	100	M	B
E.19	ERRORES	Divulgación de la información	1	PF	1	B	MB
E.21	ERRORES	Errores de mantenimiento / actualización de programas (software)	1	PF	100	M	B
A.7	ATAQUES	Uso no previsto	1	PF	1	B	MB
A.11	ATAQUES	Acceso no autorizado	1	PF	1	B	MB
A.16	ATAQUES	Introducción de información falsa	1	PF	100	M	B
A.17	ATAQUES	Corrupción de la información	1	PF	100	M	B
A.18	ATAQUES	Destrucción de la información	1	PF	100	M	B
A.19	ATAQUES	Divulgación de la información	1	PF	1	B	MB

D	CONF	Datos de configuración	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.2	ERRORES	Errores del administrador	2	FN	100	B	B
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	MB	MB
E.4	ERRORES	Errores de Configuración	2	FN	100	B	B
E.7	ERRORES	Deficiencias en la organización	2	FN	10	MB	MB
E.15	ERRORES	Alteración de la información	2	FN	100	B	B
E.16	ERRORES	Introducción de información incorrecta	2	FN	100	B	B
E.17	ERRORES	Degradación de la Información	1	PF	100	B	MB
E.18	ERRORES	Destrucción de la información	1	PF	100	B	MB
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	B	MB
A.5	ATAQUES	Suplantación de la identidad del usuario	1	PF	1	MB	MB
A.6	ATAQUES	Abuso de privilegios de acceso	1	PF	100	B	MB
A.11	ATAQUES	Acceso no autorizado	1	PF	100	B	MB
A.15	ATAQUES	Modificación de la Información	1	PF	100	B	MB
A.16	ATAQUES	Introducción de información falsa	1	PF	100	B	MB
A.17	ATAQUES	Corrupción de la información	1	PF	100	B	MB
A.18	ATAQUES	Destrucción de la información	1	PF	100	B	MB
A.19	ATAQUES	Divulgación de la información	1	PF	1	MB	MB

D	PASSWORD	Credenciales de usuario	M

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.1	ERRORES	Errores de los usuarios	2	FN	1	B	B
E.2	ERRORES	Errores del administrador	2	FN	100	M	M
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	B	B
E.4	ERRORES	Errores de Configuración	2	FN	100	M	M
E.7	ERRORES	Deficiencias en la organización	2	FN	10	B	B
E.8	ERRORES	Difusión de software dañino	1	PF	10	B	MB
E.15	ERRORES	Alteración de la información	2	FN	100	M	M
E.16	ERRORES	Introducción de información incorrecta	2	FN	100	M	M
E.17	ERRORES	Degradación de la Información	1	PF	100	M	B
E.18	ERRORES	Destrucción de la información	1	PF	100	M	B
E.19	ERRORES	Divulgación de la información	1	PF	100	M	B
E.20	ERRORES	Vulnerabilidades de los programas (software)	1	PF	10	B	MB
A.5	ATAQUES	Suplantación de la identidad del usuario	1	PF	100	M	B
A.6	ATAQUES	Abuso de privilegios de acceso	1	PF	100	M	B
A.7	ATAQUES	Uso no previsto	1	PF	10	B	MB
A.8	ATAQUES	Difusión de software dañino	1	PF	10	B	MB
A.14	ATAQUES	Interceptación de información (escucha)	1	PF	100	M	B
A.15	ATAQUES	Modificación de la Información	1	PF	100	M	B
A.16	ATAQUES	Introducción de información falsa	1	PF	100	M	B
A.17	ATAQUES	Corrupción de la información	1	PF	100	M	B
A.18	ATAQUES	Destrucción de la información	1	PF	100	M	B
A.19	ATAQUES	Divulgación de la información	1	PF	100	M	B

D	AUTH	datos de validación de credenciales	M

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.1	ERRORES	Errores de los usuarios	1	PF	1	B	MB
E.2	ERRORES	Errores del administrador	2	FN	100	M	M
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	B	B
E.4	ERRORES	Errores de Configuración	2	FN	100	M	M
E.7	ERRORES	Deficiencias en la organización	2	FN	10	B	B
E.8	ERRORES	Difusión de software dañino	1	PF	10	B	MB
E.15	ERRORES	Alteración de la información	2	FN	100	M	M
E.16	ERRORES	Introducción de información incorrecta	2	FN	100	M	M
E.17	ERRORES	Degradación de la Información	1	PF	100	M	B
E.18	ERRORES	Destrucción de la información	1	PF	100	M	B
E.19	ERRORES	Divulgación de la información	1	PF	100	M	B
E.20	ERRORES	Vulnerabilidades de los programas (software)	1	PF	10	B	MB
A.5	ATAQUES	Suplantación de la identidad del usuario	1	PF	1	B	MB
A.6	ATAQUES	Abuso de privilegios de acceso	1	PF	100	M	B
A.7	ATAQUES	Uso no previsto	1	PF	10	B	MB
A.8	ATAQUES	Difusión de software dañino	1	PF	10	B	MB
A.14	ATAQUES	Interceptación de información (escucha)	1	PF	100	M	B
A.15	ATAQUES	Modificación de la Información	1	PF	100	M	B
A.16	ATAQUES	Introducción de información falsa	1	PF	100	M	B
A.17	ATAQUES	Corrupción de la información	1	PF	100	M	B
A.18	ATAQUES	Destrucción de la información	1	PF	100	M	B
A.19	ATAQUES	Divulgación de la información	1	PF	10	B	MB

D	ACL	datos de control de acceso	M

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.2	ERRORES	Errores del administrador	2	FN	100	M	M
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	B	B
E.4	ERRORES	Errores de Configuración	2	FN	100	M	M
E.7	ERRORES	Deficiencias en la organización	2	FN	10	B	B
E.8	ERRORES	Difusión de software dañino	1	PF	10	B	MB
E.15	ERRORES	Alteración de la información	2	FN	100	M	M
E.16	ERRORES	Introducción de información incorrecta	2	FN	100	M	M
E.17	ERRORES	Degradación de la Información	1	PF	100	M	B
E.18	ERRORES	Destrucción de la información	1	PF	100	M	B
E.19	ERRORES	Divulgación de la información	1	PF	10	B	MB
E.20	ERRORES	Vulnerabilidades de los programas (software)	1	PF	10	B	MB
A.5	ATAQUES	Suplantación de la identidad del usuario	1	PF	10	B	MB
A.6	ATAQUES	Abuso de privilegios de acceso	1	PF	100	M	B
A.7	ATAQUES	Uso no previsto	1	PF	10	B	MB
A.8	ATAQUES	Difusión de software dañino	1	PF	10	B	MB
A.14	ATAQUES	Interceptación de información (escucha)	1	PF	10	B	MB
A.15	ATAQUES	Modificación de la Información	1	PF	100	M	B
A.16	ATAQUES	Introducción de información falsa	1	PF	100	M	B
A.17	ATAQUES	Corrupción de la información	1	PF	100	M	B
A.18	ATAQUES	Destrucción de la información	1	PF	100	M	B
A.19	ATAQUES	Divulgación de la información	1	PF	10	B	MB

D	LOG	registro de actividad	A

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.2	ERRORES	Errores del administrador	2	FN	100	A	A
E.3	ERRORES	Errores de monitorización (log)	2	FN	100	A	A
E.4	ERRORES	Errores de Configuración	2	FN	100	A	A
E.8	ERRORES	Difusión de software dañino	1	PF	100	A	M
E.15	ERRORES	Alteración de la información	1	PF	100	A	M
E.16	ERRORES	Introducción de información incorrecta	1	PF	100	A	M
E.17	ERRORES	Degradación de la Información	1	PF	100	A	M
E.18	ERRORES	Destrucción de la información	1	PF	100	A	M
E.19	ERRORES	Divulgación de la información	1	PF	100	A	M
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	A	M
A.5	ATAQUES	Suplantación de la identidad del usuario	4	MF	100	A	MA
A.6	ATAQUES	Abuso de privilegios de acceso	1	PF	100	A	M
A.7	ATAQUES	Uso no previsto	1	PF	10	M	B
A.14	ATAQUES	Interceptación de información (escucha)	1	PF	10	M	B
A.15	ATAQUES	Modificación de la Información	1	PF	100	A	M
A.16	ATAQUES	Introducción de información falsa	1	PF	100	A	M
A.17	ATAQUES	Corrupción de la información	1	PF	100	A	M
A.18	ATAQUES	Destrucción de la información	1	PF	100	A	M
A.19	ATAQUES	Divulgación de la información	1	PF	10	M	B

D	EXE	código ejecutable	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.2	ERRORES	Errores del administrador	1	PF	100	B	MB
E.3	ERRORES	Errores de monitorización (log)	1	PF	10	MB	MB
E.4	ERRORES	Errores de Configuración	1	PF	100	B	MB
E.8	ERRORES	Difusión de software dañino	4	MF	10	MB	M
E.20	ERRORES	Vulnerabilidades de los programas (software)	2	FN	10	MB	MB
E.21	ERRORES	Errores de mantenimiento / actualización de programas (software)	2	FN	100	B	B
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	B	MB
A.6	ATAQUES	Abuso de privilegios de acceso	1	PF	100	B	MB
A.7	ATAQUES	Uso no previsto	1	PF	100	B	MB
A.8	ATAQUES	Difusión de software dañino	1	PF	10	MB	MB

D	TEST	datos de prueba	B

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.2	ERRORES	Errores del administrador	2	FN	100	B	B
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	MB	MB
E.4	ERRORES	Errores de Configuración	2	FN	100	B	B
E.15	ERRORES	Alteración de la información	2	FN	100	B	B
E.18	ERRORES	Destrucción de la información	2	FN	100	B	B

O	O	Objetivos y Misión	A

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA	DEGRADACIÓN		IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	A	M
N.2	DESASTRES NATURALES	Daños por agua	1	PF	100	A	M
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	100	A	M
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	A	M
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	A	M
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	2	FN	100	A	A
I.6	DESASTRES INDUSTRIALES	Corte de Suministro Electrico	1	PF	100	A	M
I.7	DESASTRES INDUSTRIALES	Condiciones inadecuadas de temperatura y/o humedad	1	PF	100	A	M
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	A	A
I.9	DESASTRES INDUSTRIALES	Interrupción de otros servicios y suministros esenciales	2	FN	100	A	A
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	100	A	M
E.1	ERRORES	Errores de los usuarios	2	FN	1	M	M
E.2	ERRORES	Errores del administrador	2	FN	100	A	A
E.3	ERRORES	Errores de monitorización (log)	2	FN	10	M	M
E.4	ERRORES	Errores de Configuración	2	FN	100	A	A
E.7	ERRORES	Deficiencias en la organización	2	FN	10	M	M
E.8	ERRORES	Difusión de software dañino	4	MF	10	M	MA
E.14	ERRORES	Escapes de información	4	MF	100	A	MA
E.15	ERRORES	Alteración de la información	4	MF	100	A	MA
E.16	ERRORES	Introducción de información incorrecta	4	MF	100	A	MA
E.17	ERRORES	Degradación de la Información	1	PF	100	A	M
E.18	ERRORES	Destrucción de la información	1	PF	100	A	M
E.19	ERRORES	Divulgación de la información	4	MF	100	A	MA

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.20	ERRORES	Vulnerabilidades de los programas (software)	2	FN	10	M	M
E.21	ERRORES	Errores de mantenimiento / actualización de programas (software)	2	FN	10	M	M
E.23	ERRORES	Errores de mantenimiento / actualización de equipos (hardware)	2	FN	10	M	M
E.24	ERRORES	Caida del sistema por agotamiento de recursos	1	PF	100	A	M
E.28	ERRORES	Indisponibilidad del personal	3	F	10	M	A
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	A	M
A.5	ATAQUES	Suplantación de la identidad del usuario	1	PF	100	A	M
A.6	ATAQUES	Abuso de privilegios de acceso	1	PF	100	A	M
A.7	ATAQUES	Uso no previsto	1	PF	100	A	M
A.8	ATAQUES	Difusión de software dañino	1	PF	10	M	B
A.13	ATAQUES	Repudio	1	PF	10	M	B
A.14	ATAQUES	Interceptación de información (escucha)	1	PF	100	A	M
A.15	ATAQUES	Modificación de la Información	1	PF	100	A	M
A.16	ATAQUES	Introducción de información falsa	1	PF	100	A	M
A.17	ATAQUES	Corrupción de la información	1	PF	100	A	M
A.18	ATAQUES	Destrucción de la información	1	PF	100	A	M
A.19	ATAQUES	Divulgación de la información	1	PF	100	A	M
A.22	ATAQUES	Manipulación de los programas	1	PF	10	M	B
A.24	ATAQUES	Denegación de Servicio	1	PF	100	A	M
A.25	ATAQUES	Robo	2	FN	10	M	M
A.26	ATAQUES	Ataque Destructivo	1	PF	10	M	B
A.28	ATAQUES	Indisponibilidad del personal	1	PF	100	A	M
A.29	ATAQUES	Extorsion	1	PF	10	M	B
A.30	ATAQUES	Ingenieria social	3	F	10	M	A

IMG	IMG	Imagen, reputación, credibilidad	A

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA	DEGRADACIÓN		IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	1	M	B
N.2	DESASTRES NATURALES	Daños por agua	1	PF	1	M	B
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	1	M	B
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	A	M
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	A	M
I.5	DESASTRES INDUSTRIALES	Averia de origen Físico o Lógico	3	F	100	A	MA
I.6	DESASTRES INDUSTRIALES	Corte de Suministro Electrico	1	PF	100	A	M
I.7	DESASTRES INDUSTRIALES	Condiciones inadecuadas de temperatura y/o humedad	1	PF	100	A	M
I.8	DESASTRES INDUSTRIALES	Fallo de servicios de comunicaciones	2	FN	100	A	A
I.9	DESASTRES INDUSTRIALES	Interrupción de otros servicios y suministros esenciales	2	FN	100	A	A
I.+	DESASTRES INDUSTRIALES	Otros desastres Industriales	1	PF	100	A	M
E.1	ERRORES	Errores de los usuarios	2	FN	100	A	A
E.2	ERRORES	Errores del administrador	2	FN	100	A	A
E.3	ERRORES	Errores de monitorización (log)	2	FN	100	A	A
E.4	ERRORES	Errores de Configuración	2	FN	100	A	A
E.7	ERRORES	Deficiencias en la organización	2	FN	100	A	A
E.8	ERRORES	Difusión de software dañino	4	MF	10	M	MA
E.14	ERRORES	Escapes de información	4	MF	100	A	MA
E.15	ERRORES	Alteración de la información	4	MF	100	A	MA
E.16	ERRORES	Introducción de información incorrecta	4	MF	100	A	MA
E.17	ERRORES	Degradación de la Información	1	PF	100	A	M
E.18	ERRORES	Destrucción de la información	1	PF	100	A	M
E.19	ERRORES	Divulgación de la información	4	MF	100	A	MA

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.20	ERRORES	Vulnerabilidades de los programas (software)	2	FN	10	M	M
E.21	ERRORES	Errores de mantenimiento / actualización de programas (software)	2	FN	100	A	A
E.23	ERRORES	Errores de mantenimiento / actualización de equipos (hardware)	2	FN	100	A	A
E.24	ERRORES	Caida del sistema por agotamiento de recursos	1	PF	100	A	M
E.28	ERRORES	Indisponibilidad del personal	3	F	100	A	**MA**
A.4	ATAQUES	Manipulación de la configuración	1	PF	100	A	M
A.5	ATAQUES	Suplantación de la identidad del usuario	4	MF	10	M	**MA**
A.6	ATAQUES	Abuso de privilegios de acceso	1	PF	10	M	B
A.7	ATAQUES	Uso no previsto	1	PF	100	A	M
A.8	ATAQUES	Difusión de software dañino	4	MF	10	M	**MA**
A.13	ATAQUES	Repudio	1	PF	100	A	M
A.14	ATAQUES	Interceptación de información (escucha)	1	PF	100	A	M
A.15	ATAQUES	Modificación de la Información	1	PF	100	A	M
A.16	ATAQUES	Introducción de información falsa	1	PF	100	A	M
A.17	ATAQUES	Corrupción de la información	1	PF	100	A	M
A.18	ATAQUES	Destrucción de la información	1	PF	100	A	M
A.19	ATAQUES	Divulgación de la información	1	PF	100	A	M
A.22	ATAQUES	Manipulación de los programas	1	PF	10	M	B
A.24	ATAQUES	Denegación de Servicio	1	PF	100	A	M
A.25	ATAQUES	Robo	1	PF	100	A	M
A.26	ATAQUES	Ataque Destructivo	1	PF	100	A	M
A.28	ATAQUES	Indisponibilidad del personal	1	PF	100	A	M
A.29	ATAQUES	Extorsion	1	PF	10	M	B
A.30	ATAQUES	Ingenieria social	3	F	10	M	A

KNW	KNW	Conocimiento acumulado	A

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.28	ERRORES	Indisponibilidad del personal	2	FN	100	A	A
A.28	ATAQUES	Indisponibilidad del personal	2	FN	100	A	A

IP	IP	Intimidad / Honor de las personas	A

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
E.7	ERRORES	Deficiencias en la organización	3	F	100	A	**MA**
E.14	ERRORES	Escapes de información	4	MF	100	A	**MA**
A.5	ATAQUES	Suplantación de la identidad del usuario	4	MF	100	A	**MA**
A.6	ATAQUES	Abuso de privilegios de acceso	1	PF	100	A	M
A.11	ATAQUES	Acceso no autorizado	1	PF	100	A	M
A.14	ATAQUES	Interceptación de información (escucha)	1	PF	100	A	M
A.19	ATAQUES	Divulgación de la información	1	PF	100	A	M
A.29	ATAQUES	Extorsion	1	PF	10	M	B
A.30	ATAQUES	Ingenieria social	3	F	10	M	A

IF	IF	Integridad Fisica de las personas	MA

ID AMENAZA	ORIGEN AMENAZA	AMENAZA	FRECUENCIA		DEGRADACIÓN	IMPACTO POTENCIAL	RIESGO POTENCIAL
N.1	DESASTRES NATURALES	Fuego	1	PF	100	MA	A
N.2	DESASTRES NATURALES	Daños por agua	1	PF	100	MA	A
N.+	DESASTRES NATURALES	Otros desastres naturales	1	PF	100	MA	A
I.1	DESASTRES INDUSTRIALES	Fuego	1	PF	100	MA	A
I.2	DESASTRES INDUSTRIALES	Daños por agua	1	PF	100	MA	A
E.1	ERRORES	Errores de los usuarios	4	MF	100	MA	**MA**
E.2	ERRORES	Errores del administrador	4	MF	100	MA	**MA**
E.3	ERRORES	Errores de monitorización (log)	4	MF	100	MA	**MA**
E.4	ERRORES	Errores de Configuración	4	MF	100	MA	**MA**
E.7	ERRORES	Deficiencias en la organización	4	MF	100	MA	**MA**
E.16	ERRORES	Introducción de información incorrecta	4	MF	100	MA	**MA**
E.17	ERRORES	Degradación de la Información	1	PF	100	MA	A
E.18	ERRORES	Destrucción de la información	3	F	100	MA	**MA**
E.28	ERRORES	Indisponibilidad del personal	2	FN	100	MA	**MA**
A.15	ATAQUES	Modificación de la Información	1	PF	100	MA	A
A.16	ATAQUES	Introducción de información falsa	1	PF	100	MA	A
A.17	ATAQUES	Corrupción de la información	1	PF	100	MA	A
A.18	ATAQUES	Destrucción de la información	1	PF	100	MA	A
A.24	ATAQUES	Denegación de Servicio	1	PF	100	MA	A
A.26	ATAQUES	Ataque Destructivo	1	PF	100	MA	A

17. Anexo X. Salvaguardas, Impacto Residual y Riesgo Residual

HW SWITCH conmutadores A

ID	AMENAZA	F	D	I P	R P	SV	DESCRIPCION	L	E	R D	D R	R F	I R	R R
I.5	Averia de origen Físico o Lógico	FN	100	A	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.6	Corte de Suministro Electrico	FN	100	A	A	MN	De Monitorización	L4	0,95	5	1	PF	M	B
I.8	Fallo de servicios de comunicaciones	FN	100	A	A	DC	De Detección	L4	0,95	5	1	PF	M	B
E.2	Errores del administrador	FN	100	A	A	AW	De Concienciación	L2	0,5	50	50	PF	A	M
E.3	Errores de monitorización (log)	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M
E.4	Errores de Configuración	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M

HW FIREWALL cortafuegos A

ID	AMENAZA	F	D	I P	R P	SV	DESCRIPCION	L	E	R D	D R	R F	I R	R R
I.5	Averia de origen Físico o Lógico	FN	100	A	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.8	Fallo de servicios de comunicaciones	FN	100	A	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
E.2	Errores del administrador	FN	100	A	A	AW	De Concienciación	L2	0,5	50	50	PF	A	M
E.3	Errores de monitorización (log)	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M
E.4	Errores de Configuración	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M
E.23	Errores de mantenimiento / actualización de equipos (hardware)	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M
A.26	Ataque Destructivo	MF	100	A	MA	DC	De Detección	L3	0,9	10	10	F	M	A

MEDIA SAN almacenamiento en red MA

ID	AMENAZA	F	D	I P	R P	SV	DESCRIPCION	L	E	R D	D R	R F	I R	R R
N.1	Fuego	PF	100	MA	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
N.2	Daños por agua	PF	100	MA	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
N.+	Otros desastres naturales	PF	100	MA	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.1	Fuego	PF	100	MA	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.2	Daños por agua	PF	100	MA	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.4	Contaminación Electromagnética	PF	100	MA	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.5	Averia de origen Físico o Lógico	PF	100	MA	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.6	Corte de Suministro Electrico	PF	100	MA	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.7	Condiciones inadecuadas de temperatura y/o humedad	PF	100	MA	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.8	Fallo de servicios de comunicaciones	FN	100	MA	**MA**	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.10	Degradación de los soportes de almacenamiento de la información	PF	100	MA	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.+	Otros desastres Industriales	PF	100	MA	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
E.2	Errores del administrador	FN	100	MA	**MA**	AW	De Concienciación	L2	0,5	50	50	PF	MA	A
E.3	Errores de monitorización (log)	FN	10	A	A	MN	De Monitorización	L2	0,5	5	1	PF	M	B
E.4	Errores de Configuración	FN	100	MA	**MA**	MN	De Monitorización	L2	0,5	50	50	PF	MA	A
A.4	Manipulación de la configuración	PF	100	MA	A	DC	De Detección	L3	0,9	10	10	PF	A	M
A.25	Robo	PF	100	MA	A	DR	Disuasorias	L3	0,9	10	10	PF	A	M
A.26	Ataque Destructivo	PF	100	MA	A	DC	De Detección	L3	0,9	10	10	PF	A	M
A.28	Indisponibilidad del personal	PF	100	MA	A	IM	Minimizadoras	L2	0,5	50	50	PF	MA	A

SW WWW servidor de presentación A

ID	AMENAZA	F	D	I P	R P	SV	DESCRIPCION	L	E	R D	D R	R F	I R	R R
I.5	Averia de origen Físico o Lógico	FN	100	A	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.8	Fallo de servicios de comunicaciones	FN	100	A	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
E.2	Errores del administrador	FN	100	A	A	AW	De Concienciación	L2	0,5	50	50	PF	A	M
E.4	Errores de Configuración	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M
E.8	Difusión de software dañino	MF	10	M	MA	DC	De Detección	L3	0,9	1	1	F	M	A
E.21	Errores de mantenimiento / actualización de programas (software)	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M

SW APP servidor de aplicaciones A

ID	AMENAZA	F	D	I P	R P	SV	DESCRIPCION	L	E	R D	D R	R F	I R	R R
I.5	Averia de origen Físico o Lógico	FN	100	A	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.8	Fallo de servicios de comunicaciones	FN	100	A	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
E.2	Errores del administrador	FN	100	A	A	AW	De Concienciación	L2	0,5	50	50	PF	A	M
E.4	Errores de Configuración	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M
E.8	Difusión de software dañino	MF	10	M	MA	DC	De Detección	L3	0,9	1	1	F	M	A
E.21	Errores de mantenimiento / actualización de programas (software)	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M

SW DBMS sistema de gestión de bases de datos A

ID	AMENAZA	F	D	I P	R P	SV	DESCRIPCION	L	E	R D	D R	R F	I R	R R
I.5	Averia de origen Físico o Lógico	FN	100	A	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.8	Fallo de servicios de comunicaciones	FN	100	A	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
E.2	Errores del administrador	FN	100	A	A	AW	De Concienciación	L2	0,5	50	50	PF	A	M
E.4	Errores de Configuración	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M
E.8	Difusión de software dañino	MF	10	M	MA	DC	De Detección	L3	0,9	1	1	F	M	A
E.21	Errores de mantenimiento / actualización de programas (software)	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M

SW OS sistema operativo A

ID	AMENAZA	F	D	I P	R P	SV	DESCRIPCION	L	E	R D	D R	R F	I R	R R
I.5	Averia de origen Físico o Lógico	FN	100	A	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.8	Fallo de servicios de comunicaciones	FN	100	A	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
E.2	Errores del administrador	FN	100	A	A	AW	De Concienciación	L2	0,5	50	50	PF	A	M
E.4	Errores de Configuración	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M
E.8	Difusión de software dañino	MF	10	M	MA	DC	De Detección	L3	0,9	1	1	F	M	A
E.21	Errores de mantenimiento / actualización de programas (software)	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M
E.24	Caida del sistema por agotamiento de recursos	FN	100	A	A	RC	Recuperativas	L0	0	100	100	FN	A	A

SW HYPERVISOR gestor de máquinas virtuales A

ID	AMENAZA	F	D	I P	R P	SV	DESCRIPCION	L	E	R D	D R	R F	I R	R R
I.5	Averia de origen Físico o Lógico	FN	100	A	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.8	Fallo de servicios de comunicaciones	FN	100	A	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
E.2	Errores del administrador	FN	100	A	A	AW	De Concienciación	L2	0,5	50	50	PF	A	M
E.4	Errores de Configuración	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M
E.8	Difusión de software dañino	MF	10	M	MA	DC	De Detección	L3	0,9	1	1	F	M	A
E.21	Errores de mantenimiento / actualización de programas (software)	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M

SW TS servidor de terminales A

ID	AMENAZA	F	D	I P	R P	SV	DESCRIPCION	L	E	R D	D R	R F	I R	R R
I.5	Averia de origen Físico o Lógico	FN	100	A	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.8	Fallo de servicios de comunicaciones	FN	100	A	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
E.2	Errores del administrador	FN	100	A	A	AW	De Concienciación	L2	0,5	50	50	PF	A	M
E.4	Errores de Configuración	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M
E.8	Difusión de software dañino	MF	10	M	MA	DC	De Detección	L3	0,9	1	1	F	M	A
E.21	Errores de mantenimiento / actualización de programas (software)	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M

D PERA Datos de carácter personal nivel alto A

ID	AMENAZA	F	D	I P	R P	SV	DESCRIPCION	L	E	R D	D R	R F	I R	R R
E.1	Errores de los usuarios	MF	100	A	MA	AW	De Concienciación	L2	0,5	50	50	F	A	MA
E.2	Errores del administrador	FN	100	A	A	AW	De Concienciación	L2	0,5	50	50	PF	A	M
E.7	Deficiencias en la organización	FN	50	A	A	AD	Administrativas	L1	0,1	45	50	FN	A	A
E.15	Alteración de la información	MF	100	A	MA	CR	Correctivas	L1	0,1	90	100	MF	A	MA
E.16	Introducción de información incorrecta	MF	100	A	MA	CR	Correctivas	L1	0,1	90	100	MF	A	MA
E.19	Divulgación de la información	MF	10	M	MA	AW	De Concienciación	L2	0,5	5	1	F	M	A
A.5	Suplantación de la identidad del usuario	MF	1	M	MA	AW	De Concienciación	L2	0,5	0,5	1	F	M	A
A.7	Uso no previsto	F	10	M	A	AW	De Concienciación	L2	0,5	5	1	FN	M	M

D LOG registro de actividad A

ID	AMENAZA	F	D	I P	R P	SV	DESCRIPCION	L	E	R D	D R	R F	I R	R R
E.2	Errores del administrador	FN	100	A	A	AW	De Concienciación	L2	0,5	50	50	PF	A	M
E.3	Errores de monitorización (log)	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M
E.4	Errores de Configuración	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M
A.5	Suplantación de la identidad del usuario	MF	100	A	MA	AW	De Concienciación	L2	0,5	50	50	F	A	MA

O O Objetivos y Misión A

ID	AMENAZA	F	D	I P	R P	SV	DESCRIPCION	L	E	R D	D R	R F	I R	R R
I.5	Averia de origen Físico o Lógico	FN	100	A	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.8	Fallo de servicios de comunicaciones	FN	100	A	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.9	Interrupción de otros servicios y suministros esenciales	FN	100	A	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
E.2	Errores del administrador	FN	100	A	A	AW	De Concienciación	L2	0,5	50	50	PF	A	M
E.4	Errores de Configuración	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M
E.8	Difusión de software dañino	MF	10	M	MA	DC	De Detección	L3	0,9	1	1	F	M	A
E.14	Escapes de información	MF	100	A	MA	AW	De Concienciación	L2	0,5	50	50	F	A	MA
E.15	Alteración de la información	MF	100	A	MA	CR	Correctivas	L1	0,1	90	100	MF	A	MA
E.16	Introducción de información incorrecta	MF	100	A	MA	CR	Correctivas	L1	0,1	90	100	MF	A	MA
E.19	Divulgación de la información	MF	100	A	MA	AW	De Concienciación	L2	0,5	50	50	F	A	MA
E.28	Indisponibilidad del personal	F	10	M	A	IM	Minimizadoras	L1	0,1	9	10	F	M	A
A.30	Ingenieria social	F	10	M	A	AW	De Concienciación	L2	0,5	5	1	FN	M	M

IMG IMG Imagen, reputación, credibilidad A

ID	AMENAZA	F	D	I P	R P	SV	DESCRIPCION	L	E	R D	D R	R F	I R	R R
I.5	Averia de origen Físico o Lógico	F	100	A	MA	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.8	Fallo de servicios de comunicaciones	FN	100	A	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.9	Interrupción de otros servicios y suministros esenciales	FN	100	A	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
E.1	Errores de los usuarios	FN	100	A	A	AW	De Concienciación	L2	0,5	50	50	PF	A	M
E.2	Errores del administrador	FN	100	A	A	AW	De Concienciación	L2	0,5	50	50	PF	A	M
E.3	Errores de monitorización (log)	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M
E.4	Errores de Configuración	FN	100	A	A	DC	De Detección	L3	0,9	10	10	PF	M	B
E.7	Deficiencias en la organización	FN	100	A	A	AD	Administrativas	L1	0,1	90	100	FN	A	A
E.8	Difusión de software dañino	MF	10	M	MA	DC	De Detección	L3	0,9	1	1	F	M	A
E.14	Escapes de información	MF	100	A	MA	AW	De Concienciación	L2	0,5	50	50	F	A	MA
E.15	Alteración de la información	MF	100	A	MA	CR	Correctivas	L1	0,1	90	100	MF	A	MA
E.16	Introducción de información incorrecta	MF	100	A	MA	CR	Correctivas	L1	0,1	90	100	MF	A	MA
E.19	Divulgación de la información	MF	100	A	MA	AW	De Concienciación	L2	0,5	50	50	F	A	MA
E.21	Errores de mantenimiento / actualización de programas (software)	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M
E.23	Errores de mantenimiento / actualización de equipos (hardware)	FN	100	A	A	MN	De Monitorización	L2	0,5	50	50	PF	A	M
E.28	Indisponibilidad del personal	F	100	A	MA	IM	Minimizadoras	L1	0,1	90	100	F	A	MA
A.5	Suplantación de la identidad del usuario	MF	10	M	MA	AW	De Concienciación	L2	0,5	5	1	F	M	A
A.8	Difusión de software dañino	MF	10	M	MA	DC	De Detección	L3	0,9	1	1	F	M	A
A.30	Ingenieria social	F	10	M	A	AW	De Concienciación	L2	0,5	5	1	FN	M	M

KNW KNW Conocimiento acumulado A

ID	AMENAZA	F	D	I P	R P	SV	DESCRIPCION	L	E	R D	D R	R F	I R	R R
E.28	Indisponibilidad del personal	FN	100	A	A	IM	Minimizadoras	L1	0,1	90	100	FN	A	A
A.28	Indisponibilidad del personal	FN	100	A	A	IM	Minimizadoras	L1	0,1	90	100	FN	A	A

IP IP Intimidad / Honor de las personas A

ID	AMENAZA	F	D	I P	R P	SV	DESCRIPCION	L	E	R D	D R	R F	I R	R R
E.7	Deficiencias en la organización	F	100	A	MA	AD	Administrativas	L1	0,1	90	100	F	A	MA
E.14	Escapes de información	MF	100	A	MA	AW	De Concienciación	L2	0,5	50	50	F	A	MA
A.5	Suplantación de la identidad del usuario	MF	100	A	MA	AW	De Concienciación	L2	0,5	50	50	F	A	MA
A.30	Ingenieria social	F	10	M	A	AW	De Concienciación	L2	0,5	5	1	FN	M	M

IF IF Integridad Fisica de las personas MA

ID	AMENAZA	F	D	I P	R P	SV	DESCRIPCION	L	E	R D	D R	R F	I R	R R
N.1	Fuego	PF	100	MA	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
N.2	Daños por agua	PF	100	MA	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
N.+	Otros desastres naturales	PF	100	MA	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.1	Fuego	PF	100	MA	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
I.2	Daños por agua	PF	100	MA	A	PR	Preventivas	L4	0,95	5	1	PF	M	B
E.1	Errores de los usuarios	MF	100	MA	MA	AW	De Concienciación	L2	0,5	50	50	F	MA	MA
E.2	Errores del administrador	MF	100	MA	MA	AW	De Concienciación	L2	0,5	50	50	F	MA	MA
E.3	Errores de monitorización (log)	MF	100	MA	MA	MN	De Monitorización	L2	0,5	50	50	F	MA	MA
E.4	Errores de Configuración	MF	100	MA	MA	DC	De Detección	L3	0,9	10	10	F	A	MA
E.7	Deficiencias en la organización	MF	100	MA	MA	AD	Administrativas	L1	0,1	90	100	MF	MA	MA
E.16	Introducción de información incorrecta	MF	100	MA	MA	CR	Correctivas	L1	0,1	90	100	MF	MA	MA
E.17	Degradación de la Información	PF	100	MA	A	DC	De Detección	L3	0,9	10	10	PF	A	M
E.18	Destrucción de la información	F	100	MA	MA	DC	De Detección	L3	0,9	10	10	FN	A	A
E.28	Indisponibilidad del personal	FN	100	MA	MA	IM	Minimizadoras	L1	0,1	90	100	FN	MA	MA
A.15	Modificación de la Información	PF	100	MA	A	DC	De Detección	L3	0,9	10	10	PF	A	M
A.16	Introducción de información falsa	PF	100	MA	A	DC	De Detección	L3	0,9	10	10	PF	A	M
A.17	Corrupción de la información	PF	100	MA	A	DC	De Detección	L3	0,9	10	10	PF	A	M
A.18	Destrucción de la información	PF	100	MA	A	DC	De Detección	L3	0,9	10	10	PF	A	M
A.24	Denegación de Servicio	PF	100	MA	A	RC	Recuperativas	L1	0,1	90	100	PF	MA	A
A.26	Ataque Destructivo	PF	100	MA	A	PR	Preventivas	L4	0,95	5	1	PF	M	B

Leyenda del encabezado

Sigla	Descripción
ID	Código Amenaza
AMENAZA	Descripción Amenaza
F	Frecuencia de Ocurrencia
D	Degradación
I P	Impacto Potencial
R P	Riesgo Potencial
SV	Salvaguardas
DESCRIPCION	Descripción Salvaguardas
L	Nivel Madurez Salvaguardas
E	Efectividad de las Salvaguardas
R D	Reducción de la Degradación
D R	Degradación Residual
R F	Reducción de la Frecuencia
I R	Impacto Residual
R R	Riesgo Residual

18. Anexo XI. Propuestas de Proyectos de Mejora

Inciativa: **Plan de Formación**			PROYECTO: **Concienciación a usuarios y profesionales TIC**		
CODIGO	FECHA CREACION	FECHA REVISION	REV	COORDINACIÓN	DESARROLLO/ IMPLANTACIÓN
PR-1A	lun 01/02/16		1.0	Formación	Expertos Externos
DURACION	4 semanas	FECHA INICIO	26/02/16	PRESUPUESTO:	12.000 €

OBJETIVOS	Concienciación y formación de los profesionales TIC y profesionales de Atención en Urgencias
DESCRIPCION	Cursos de concienciación especializados dirigidos a los profesionales en los que se presentan los principios legales de la protección de datos en relación con la legislación sanitaria. La concienciación estará especialmente dirigida a disminuir las amenazas Divulgación de la información, Errores de los usuarios, Errores del administrador, Escapes de información y Suplantación de la identidad del usuario
BENEFICIOS	Se espera una reducción principalmente en los riesgos que afectan a la intimidad de los pacientes y la imagen y reputación de la organización relacionados con el principal activo de la organización, los datos de carácter personal de nivel alto, pero también con los registros de actividad (LOG), y los Objetivos y Misión de la organización, su Imagen, reputación y credibilidad, la Intimidad y el honor de las personas, así como su integridad física (seguridad del paciente)
INDICADORES	• Porcentaje de alumnos asistentes al curso • Porcentaje de alumnos que superan las pruebas de evaluación.

RIESGO A MITIGAR	**Riesgo**	**Acción**	**Riesgo Actual**	**Riesgo Objetivo**
	Divulgación de la información	REDUCIR	A/MA	M
	Errores de los usuarios	REDUCIR	MA	M
	Errores del administrador	REDUCIR	A/MA	M
	Escapes de información	REDUCIR	MA	M
	Suplantación de la identidad del usuario	REDUCIR	A/MA	M

Inciativa: **Plan de Formación**			PROYECTO: **Formación a profesionales TIC (gestión de sistemas IDS/IPS)**		
CODIGO	FECHA CREACION	FECHA REVISION	REV	COORDINACIÓN	DESARROLLO/ IMPLANTACIÓN
PR-1B	lun 29/02/16		1.0	Formación	Expertos Externos
DURACION	1 semanas	FECHA INICIO	04/03/16	PRESUPUESTO:	4.500 €
OBJETIVOS	Formación de los profesionales TIC en la implementación y gestión de sistemas IDS/IPS				
DESCRIPCION	Cursos técnicos especializados sobre tecnología IDS/IPS. Especialización en sistemas adquiridos para el plan director de seguridad de la información				
BENEFICIOS	Reducción de problemas relacionados con la difusión de software dañino que pueden afectar a la disponibilidad de los sistemas de información. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la Difusión del Software Dañino.				
INDICADORES	• Porcentaje de alumnos asistentes al curso • Porcentaje de alumnos que superan las pruebas de evaluación.				
RIESGO A MITIGAR	**Riesgo**		**Acción**	**Riesgo Actual**	**Riesgo Objetivo**
	Difusión del Software Dañino		REDUCIR	A	M

Inciativa: **Plan de Formación**			PROYECTO: **Formación a profesionales TIC sobre las metodologías para la gestión de incidentes**		
CODIGO	FECHA CREACION	FECHA REVISION	REV	COORDINACIÓN	DESARROLLO/ IMPLANTACIÓN
PR-1C	lun 07/03/16		1.0	Formación	Expertos Externos
DURACION	1 semanas	FECHA INICIO	11/03/16	PRESUPUESTO:	3.500 €
OBJETIVOS	Formación de los profesionales TIC en el estándar ISO/IEC 27035:2011 Information technology — Security techniques — Information security incident management				
DESCRIPCION	La norma abarca los procesos de gestión de seguridad de la información de eventos, incidentes y vulnerabilidades. La norma amplía la sección de gestión de incidentes de seguridad de la información de la norma ISO / IEC 27002.				
BENEFICIOS	Reducción de problemas relacionados con la difusión de software dañino que pueden afectar a la disponibilidad de los sistemas de información. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la disponibilidad de los sistemas				
INDICADORES	• Porcentaje de alumnos asistentes al curso • Porcentaje de alumnos que superan las pruebas de evaluación.				
RIESGO A MITIGAR	**Riesgo**		**Acción**	**Riesgo Actual**	**Riesgo Objetivo**
	Difusión del Software Dañino		REDUCIR	A	M

Inciativa: **Plan de Formación**			PROYECTO: **Formación a profesionales TIC sobre las metodologías para la continuidad del negocio y la recuperación de desastres**		
CODIGO	FECHA CREACION	FECHA REVISION	REV	COORDINACIÓN	DESARROLLO/ IMPLANTACIÓN
PR-1D	lun 14/03/16		1.0	Formación	Expertos Externos
DURACION	1 semanas	FECHA INICIO	18/03/16	PRESUPUESTO:	3.500 €

OBJETIVOS	Formación de los profesionales en el estándar SO 22301:2012. Societal security — Business continuity management systems --- Requirements. ISO/TS 22318:2015 Societal security -- Business continuity management systems -- Guidelines for supply chain continuity			
DESCRIPCION	Esta norma internacional especifica los requisitos para la creación y gestión de un sistema eficaz de gestión de la Continuidad del Negocio (BCMS).			
BENEFICIOS	Tiempos de respuesta más cortos en la recuperación de los sistemas de información en caso de falta de indisponibilidad. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la disponibilidad de los sistemas			
INDICADORES	• Porcentaje de alumnos asistentes al curso • Porcentaje de alumnos que superan las pruebas de evaluación.			
RIESGO A MITIGAR	**Riesgo**	**Acción**	**Riesgo Actual**	**Riesgo Objetivo**
	Ataque Destructivo	REDUCIR	A	M
	Caida del sistema por agotamiento de recursos	REDUCIR	A	M
	Indisponibilidad del personal	REDUCIR	A/MA	M
	Deficiencias en la organización	REDUCIR	A/MA	M
	Denegación de Servicio	REDUCIR	A	M

Inciativa: **Plan de Formación**			PROYECTO: **Formación a usuarios y profesionales TIC en Seguridad del Paciente**		
CODIGO	FECHA CREACION	FECHA REVISION	REV	COORDINACIÓN	DESARROLLO/ IMPLANTACIÓN
PR-1E	lun 21/03/16		1.0	Formación	Expertos Externos
DURACION	1 semanas	FECHA INICIO	25/03/16	PRESUPUESTO:	3.500 €

OBJETIVOS	Concienciación y Formación de los profesionales TIC y profesionales de atención en urgencias en la identificación de eventos adversos provocados en la salud del paciente			
DESCRIPCION	Es necesario que los profesionales aprendan a identificar las posibles causas de los eventos adversos ocasionados en la salud de los pacientes como consecuencia de un mal diseño, un mal uso o una mala monitorización de los sistemas de información sanitarios.			
BENEFICIOS	Mejora en el diseño y uso de las Tecnologías de la Información Sanitarias en relación con la Seguridad del Paciente. Disminución de Eventos adversos en la salud del paciente. Disminución en la estancia media de hospitalización, disminución de la repetición de pruebas diagnósticas innecesarias, disminución de intervenciones quirúrgicas innecesarias.			
INDICADORES	• Porcentaje de alumnos asistentes al curso • Porcentaje de alumnos que superan las pruebas de evaluación.			
RIESGO A MITIGAR	**Riesgo**	**Acción**	**Riesgo Actual**	**Riesgo Objetivo**
	Alteración de la información	REDUCIR	MA	M
	Introducción de información incorrecta	REDUCIR	MA	M
	Errores de los usuarios	REDUCIR	MA	M
	Destrucción de la información	REDUCIR	A	M

Inciativa: **Plan de Formación**			PROYECTO: **Plan de difusión de sistemas de notificación de incidentes entre los usuarios**		
CODIGO	FECHA CREACION	FECHA REVISION	REV	COORDINACIÓN	DESARROLLO/ IMPLANTACIÓN
PR-1F	lun 28/03/16		1.0	Formación	Dirección TIC
DURACION	1 semanas	FECHA INICIO	01/04/16	PRESUPUESTO:	35 horas/hombre €

OBJETIVOS	Todos los usuarios de sistemas de información sanitarios deben conocer los procedimientos para la detección y notificación de incidentes
DESCRIPCION	La detección y notificación de incidentes por parte de los usuarios resulta imprescindible para el tratamiento de todos aquellos incidentes relacionados con la seguridad del paciente y otros incidentes más técnicos relacionados con la intimidad del paciente.
BENEFICIOS	Mejora en el diseño y uso de las Tecnologías de la Información Sanitarias en relación con la Seguridad del Paciente. Disminución de Eventos adversos en la salud del paciente. Reducción de problemas relacionados con la difusión de software dañino que pueden afectar a la disponibilidad de los sistemas de información. Disminución en la estancia media de hospitalización, disminución de la repetición de pruebas diagnósticas innecesarias, disminución de intervenciones quirúrgicas innecesarias. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la disponibilidad de los sistemas
INDICADORES	• Porcentaje de profesionales informados

RIESGO A MITIGAR	**Riesgo**	**Acción**	**Riesgo Actual**	**Riesgo Objetivo**
	Errores de los usuarios	REDUCIR	MA	M
	Errores del administrador	REDUCIR	MA	M
	Errores de monitorización (log)	REDUCIR	MA	M
	Errores de Configuración	REDUCIR	MA	M
	Deficiencias en la organización	REDUCIR	MA	M
	Introducción de información incorrecta	REDUCIR	MA	M
	Destrucción de la información	REDUCIR	A	M
	Indisponibilidad del personal	REDUCIR	MA	M
	Denegación de Servicio	REDUCIR	A	M
	Deficiencias en la organización	REDUCIR	A/MA	M
	Escapes de información	REDUCIR	MA	M

Inciativa: **Proyecto para la mejora de la detección, notificación y gestión de incidentes**		PROYECTO: **Planificación para la Prevención de incidentes**			
CODIGO	FECHA CREACION	FECHA REVISION	REV	COORDINACIÓN	DESARROLLO/ IMPLANTACIÓN
PR-2A	lun 04/04/16		1.0	Dirección TIC	TIC
DURACION	1 semanas	FECHA INICIO	08/04/16	PRESUPUESTO:	70 horas/hombre

OBJETIVOS	Desarrollo del plan de prevención de incidentes y creación del equipo de respuesta a incidentes.			
DESCRIPCION	Bajo la óptica de la seguridad, el primer objetivo a plantearse en una organización es reducir la probabilidad de sufrir incidentes de seguridad. Siempre que exista un incidente de seguridad, la organización sufrirá un daño que, por pequeño que sea, tendrá un impacto económico.			
BENEFICIOS	Reducción de problemas relacionados con la difusión de software dañino y otras amenazas que pueden afectar a la disponibilidad de los sistemas de información. No cuantificados. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la Difusión del Software Dañino y otras amenazas que pueden afectar a la disponibilidad de los sistemas de información.			
INDICADORES	• Plan de Prevención • Equipo de respuesta a incidentes			
RIESGO A MITIGAR	**Riesgo**	**Acción**	**Riesgo Actual**	**Riesgo Objetivo**
	Ataque Destructivo	REDUCIR	A	M
	Errores de Configuración	REDUCIR	A/MA	M
	Errores de monitorización (log)	REDUCIR	MA	M
	Difusión de software dañino	REDUCIR	A	M
	Destrucción de la información	REDUCIR	A	M
	Denegación de Servicio	REDUCIR	A	M

Inciativa: **Proyecto para la mejora de la detección, notificación y gestión de incidentes**		PROYECTO: **Planificación para la Detección y Análisis de incidentes**			
CODIGO	FECHA CREACION	FECHA REVISION	REV	COORDINACIÓN	DESARROLLO/ IMPLANTACIÓN
PR-2B	lun 11/04/16		1.0	Dirección TIC	TIC
DURACION	1 semanas	FECHA INICIO	15/04/16	PRESUPUESTO:	70 horas/hombre

OBJETIVOS	Minizar el impacto de un incidente en la organización			
DESCRIPCION	El primer paso para la correcta detección de un incidente consiste en verificar que realmente ha sucedido y, en caso afirmativo, determinar su tipo y magnitud. Identificación, análisis, evaluación inicial, determinación de la gravedad, clasificación, priorización y notificación de incidentes.			
BENEFICIOS	Reducción de problemas relacionados con la difusión de software dañino y otras amenazas que pueden afectar a la disponibilidad de los sistemas de información. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la Difusión del Software Dañino y otras amenazas que pueden afectar a la disponibilidad de los sistemas de información.			
INDICADORES	• Procedimientos de análisis y evaluación de incidentes			
RIESGO A MITIGAR	**Riesgo**	**Acción**	**Riesgo Actual**	**Riesgo Objetivo**
	Ataque Destructivo	REDUCIR	A	M
	Errores de Configuración	REDUCIR	A/MA	M
	Errores de monitorización (log)	REDUCIR	MA	M
	Difusión de software dañino	REDUCIR	A	M
	Destrucción de la información	REDUCIR	A	M
	Divulgación de la información	REDUCIR	A/MA	M
	Suplantación de la identidad del usuario	REDUCIR	A/MA	M
	Denegación de Servicio	REDUCIR	A	M

Inciativa: **Proyecto para la mejora de la detección, notificación y gestión de incidentes**		PROYECTO: **Planificación para la Contención de incidentes**			
CODIGO	FECHA CREACION	FECHA REVISION	REV	COORDINACIÓN	DESARROLLO/ IMPLANTACIÓN
PR-2C	lun 18/04/16		1.0	Dirección TIC	TIC
DURACION	1 semanas	FECHA INICIO	22/04/16	PRESUPUESTO:	70 horas/hombre

OBJETIVOS	Minizar el impacto de un incidente en la organización
DESCRIPCION	La etapa de contención puede llegar a ser muy delicada. El objetivo es contener el incidente para evitar al máximo los posibles efectos dañinos que se puedan derivar
BENEFICIOS	Reducción de problemas relacionados con la difusión de software dañino y otras amenazas que pueden afectar a la disponibilidad de los sistemas de información. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la Difusión del Software Dañino y otras amenazas que pueden afectar a la disponibilidad de los sistemas de información.
INDICADORES	• Plan de Contingencias

RIESGO A MITIGAR	**Riesgo**	**Acción**	**Riesgo Actual**	**Riesgo Objetivo**
	Ataque Destructivo	REDUCIR	A	M
	Errores de Configuración	REDUCIR	A/MA	M
	Errores de monitorización (log)	REDUCIR	MA	M
	Difusión de software dañino	REDUCIR	A	M
	Destrucción de la información	REDUCIR	A	M
	Divulgación de la información	REDUCIR	A/MA	M
	Suplantación de la identidad del usuario	REDUCIR	A/MA	M
	Denegación de Servicio	REDUCIR	A	M

Inciativa: **Proyecto para la mejora de la detección, notificación y gestión de incidentes**		PROYECTO: **Planificación para la Resolución de incidentes**			
CODIGO	FECHA CREACION	FECHA REVISION	REV	COORDINACIÓN	DESARROLLO/ IMPLANTACIÓN
PR-2D	lun 25/04/16		1.0	Dirección TIC	TIC
DURACION	1 semanas	FECHA INICIO	29/04/16	PRESUPUESTO:	70 horas/hombre

OBJETIVOS	Asegurar el libre flujo de información autorizada a través del la red y, al mismo tiempo, proteger su integridad y confidencialidad
DESCRIPCION	Sin la protección adecuada, la red es vulnerable a virus, gusanos y ataques de negación de servicio (DoS, por sus siglas en inglés) y otras amenazas internas y externas que pueden corromper el desempeño de la red, comprometer la integridad y privacidad de datos sensibles o interrumpir la continuidad del negocio. Se trata de implementar una solución de seguridad que bloquee activamente el tráfico de red sospechoso, al mismo tiempo que permite que el tráfico autorizado fluya libremente para que los usuarios puedan acceder datos y aplicaciones.
BENEFICIOS	Reducción de problemas relacionados con la difusión de software dañino y otras amenazas que pueden afectar a la disponibilidad de los sistemas de información. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la Difusión del Software Dañino y otras amenazas que pueden afectar a la disponibilidad de los sistemas de información.
INDICADORES	• Informes de alertas priorizadas • Informes de ataques prevenidos

RIESGO A MITIGAR	**Riesgo**	**Acción**	**Riesgo Actual**	**Riesgo Objetivo**
	Ataque Destructivo	REDUCIR	A	M
	Errores de Configuración	REDUCIR	A/MA	M
	Errores de monitorización (log)	REDUCIR	MA	M
	Difusión de software dañino	REDUCIR	A	M
	Destrucción de la información	REDUCIR	A	M
	Divulgación de la información	REDUCIR	A/MA	M
	Suplantación de la identidad del usuario	REDUCIR	A/MA	M
	Denegación de Servicio	REDUCIR	A	M

Inciativa: **Proyecto para la mejora de la detección, notificación y gestión de incidentes**		PROYECTO: **Implantación de sistemas IDS/IPS**			
CODIGO	FECHA CREACION	FECHA REVISION	REV	COORDINACIÓN	DESARROLLO/ IMPLANTACIÓN
PR-2E	lun 02/05/16		1.0	Dirección TIC	TIC
DURACION	1 semanas	FECHA INICIO	06/05/16	PRESUPUESTO:	12.000/año €
OBJETIVOS	Devolver los sistemas a su estado operativo y mejorar la seguridad para futuros incidentes				
DESCRIPCION	La recuperación es el proceso de devolver los sistemas afectados por el incidente a su estado operativo. También contempla la eliminación de los componentes que han provocado el incidente. Mejorar la seguridad para evitar futuros incidentes, al menos, del mismo tipo.				
BENEFICIOS	Reducción de problemas relacionados con la difusión de software dañino y otras amenazas que pueden afectar a la disponibilidad de los sistemas de información. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la Difusión del Software Dañino y otras amenazas que pueden afectar a la disponibilidad de los sistemas de información.				
INDICADORES	• Plan de recuperación de sistemas • Registro de recopilación y organización del pruebas del incidente • Registro de Valoración de daños • Procedimiento de revisión de respuesta y actualización de directivas				
RIESGO A MITIGAR	**Riesgo**		**Acción**	**Riesgo Actual**	**Riesgo Objetivo**
	Ataque Destructivo		REDUCIR	A	M
	Errores de Configuración		REDUCIR	A/MA	M
	Errores de monitorización (log)		REDUCIR	MA	M
	Difusión de software dañino		REDUCIR	A	M
	Destrucción de la información		REDUCIR	A	M
	Denegación de Servicio		REDUCIR	A	M

Inciativa: **Plan para la continuidad del negocio y recuperación de desastres**		PROYECTO: **Planificación de la Continuidad del Negocio y Recuperación de Desastres**			
CODIGO	FECHA CREACION	FECHA REVISION	REV	COORDINACIÓN	DESARROLLO/ IMPLANTACIÓN
PR-3A	lun 09/05/16		1.0	Dirección TIC	TIC
DURACION	4 semanas	FECHA INICIO	03/06/16	PRESUPUESTO:	280 horas/hombre
OBJETIVOS	Devolver los sistemas a su estado operativo y mejorar la seguridad para futuros incidentes				
DESCRIPCION	Cualquier estrategia para la recuperación de los servicios TIC despúes de un desastre debe tener en cuenta a las personas, las instalaciones y los recursos. Estos tres aspectos deben gestionarse adecuadamente para que el proceso de recuperación tenga éxito. Este proyecto detalla la estrategia de recuperación de los servicios para la Atención en Urgencias.				
BENEFICIOS	Reducción de problemas relacionados con amenazas que pueden afectar a la disponibilidad de los sistemas de información. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con amenazas que pueden afectar a la disponibilidad de los sistemas de información.				
INDICADORES	• Plan de Continuidad del Negocio y Recuperación de Desastres				
RIESGO A MITIGAR	**Riesgo**		**Acción**	**Riesgo Actual**	**Riesgo Objetivo**
	Ataque Destructivo		REDUCIR	A	M
	Caida del sistema por agotamiento de recursos		REDUCIR	A/MA	M
	Destrucción de la información		REDUCIR	MA	M
	Difusión de software dañino		REDUCIR	A	M

Inciativa: **Plan para la continuidad del negocio y recuperación de desastres**		PROYECTO: **Implantación y Operación**			
CODIGO	FECHA CREACION	FECHA REVISION	REV	COORDINACIÓN	DESARROLLO/ IMPLANTACIÓN
PR-3B	lun 06/06/16		1.0	Dirección TIC	TIC
DURACION	1 semana	FECHA INICIO	10/06/16	PRESUPUESTO:	70 horas/hombre €
OBJETIVOS	Devolver los sistemas a su estado operativo y mejorar la seguridad para futuros incidentes				
DESCRIPCION	Implantación del plan desarrollado en el proyecto Planificación de la Continuidad del Negocio y Recuperación de Desastres.				
BENEFICIOS	Reducción de problemas relacionados con amenazas que pueden afectar a la disponibilidad de los sistemas de información. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con amenazas que pueden afectar a la disponibilidad de los sistemas de información.				
INDICADORES	• Informe de resultados de implantación				

RIESGO A MITIGAR	**Riesgo**	**Acción**	**Riesgo Actual**	**Riesgo Objetivo**
	Ataque Destructivo	REDUCIR	A	M
	Caida del sistema por agotamiento de recursos	REDUCIR	A/MA	M
	Destrucción de la información	REDUCIR	MA	M
	Difusión de software dañino	REDUCIR	A	M

Inciativa: **Plan para la continuidad del negocio y recuperación de desastres**		PROYECTO: **Seguimiento y Revisión**			
CODIGO	FECHA CREACION	FECHA REVISION	REV	COORDINACIÓN	DESARROLLO/ IMPLANTACIÓN
PR-3C	lun 13/06/16		1.0	Dirección TIC	TIC
DURACION	1 semana	FECHA INICIO	17/06/16	PRESUPUESTO:	70 horas/hombre €
OBJETIVOS	Supervisión y mejora del plan de continuidad de negocio.				
DESCRIPCION	Plan de supervisión, auditoría y prueba del plan de continuidad de negocio y recuperación de desastres.				
BENEFICIOS	Mejora continua de los planes de continuidad del negocio y recuperación de desastres. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con amenazas que pueden afectar a la disponibilidad de los sistemas de información				
INDICADORES	• Plan de auditoría				

RIESGO A MITIGAR	**Riesgo**	**Acción**	**Riesgo Actual**	**Riesgo Objetivo**
	Ataque Destructivo	REDUCIR	A	M
	Caida del sistema por agotamiento de recursos	REDUCIR	A/MA	M
	Destrucción de la información	REDUCIR	MA	M
	Difusión de software dañino	REDUCIR	A	M

Inciativa: **Plan de auditoría de los sistemas de información para la seguridad del paciente.**			PROYECTO: **Creación de los mecanismos organizativos para la evaluación de las tecnologías de la información y la seguridad del paciente.**		
CODIGO	FECHA CREACION	FECHA REVISION	REV	COORDINACIÓN	DESARROLLO/ IMPLANTACIÓN
PR-4A	lun 20/06/16		1.0	Comisión Seguridad	Comisión Dirección
DURACION	1 semana	FECHA INICIO	24/06/16	PRESUPUESTO:	70 horas/hombre €

OBJETIVOS	Creación de los órganos para la supervisión y mejora de las Tecnologías de la Información Saitarias desde la perspectiva de la seguridad del paciente			
DESCRIPCION	Creación del equipo multidisciplinar capaz de analizar los sistemas de información tanto desde el punto de vista tecnológico como desde el punto de vista clínico.			
BENEFICIOS	Mejora continua de los Sistemas de Información de Urgencias, Reducción de problemas relacionados con amenazas que pueden afectar a la disponibilidad de los sistemas de información. Reducción en los riesdgos que a la Misión, imagen y reputación de la organización. Disminución en la estancia media de hospitalización, disminución de la repetición de pruebas diagnósticas innecesarias, disminución de intervenciones quirúrgicas innecesarias. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la disponibilidad de los sistemas.			
INDICADORES	• Equipo multidisciplinar			
RIESGO A MITIGAR	**Riesgo**	**Acción**	**Riesgo Actual**	**Riesgo Objetivo**
	Deficiencias en la organización	REDUCIR	MA	M
	Escapes de información	REDUCIR	MA	M
	Errores de los usuarios	REDUCIR	MA	M
	Errores del administrador	REDUCIR	MA	M
	Errores de monitorización (log)	REDUCIR	MA	M
	Errores de Configuración	REDUCIR	MA	M
	Introducción de información incorrecta	REDUCIR	MA	M
	Alteración de la información	REDUCIR	MA	M

Inciativa: **Plan de auditoría de los sistemas de información para la seguridad del paciente.**		PROYECTO: **b. paciente**		**Plan de Auditoría de seguridad del**	
CODIGO	FECHA CREACION	FECHA REVISION	REV	COORDINACIÓN	DESARROLLO/ IMPLANTACIÓN
PR-4B	lun 27/06/16		1.0	Comisión Seguridad	Comisión Dirección
DURACION	1 semana	FECHA INICIO	01/07/16	PRESUPUESTO:	70 horas/hombre €

OBJETIVOS	Creación del plan de auditoría de los sistemas de información de atención en urgencias.
DESCRIPCION	Uso de las guías (SAFER), diseñadas para ayudar a los médicos y Organizaciones Sanitarias a evaluar la seguridad y eficacia de sus implementaciones de EHR, identificar áreas específicas de vulnerabilidades, y crear soluciones y cambios de cultura para mitigar los riesgos. El objetivo de las guías SAFER se basa en una evaluación de riesgos proactiva y consiste en eliminar o minimizar los riesgos de seguridad relacionados con los EHR para aumentar la resiliencia de los sistemas, que se define como "el grado en que un sistema previene, detecta, mitiga o mejora los peligros o incidentes para que una organización pueda recuperar su capacidad original para prestar la atención sanitaria
BENEFICIOS	Reducción de Eventos Adversos en la Seguridad del Paciente. Disminución en la estancia media de hospitalización, disminución de la repetición de pruebas diagnósticas innecesarias, disminución de intervenciones quirúrgicas innecesarias. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la disponibilidad de los sistemas.
INDICADORES	• Plan de auditoría de seguridad del paciente

RIESGO A MITIGAR	**Riesgo**	**Acción**	**Riesgo Actual**	**Riesgo Objetivo**
	Deficiencias en la organización	REDUCIR	MA	M
	Escapes de información	REDUCIR	MA	M
	Errores de los usuarios	REDUCIR	MA	M
	Errores del administrador	REDUCIR	MA	M
	Errores de monitorización (log)	REDUCIR	MA	M
	Errores de Configuración	REDUCIR	MA	M
	Introducción de información incorrecta	REDUCIR	MA	M
	Alteración de la información	REDUCIR	MA	M

Inciativa: **Plan de auditoría de los sistemas de información para la seguridad del paciente.**		PROYECTO: **Auditoría de Seguridad del Paciente**			
CODIGO	FECHA CREACION	FECHA REVISION	REV	COORDINACIÓN	DESARROLLO/ IMPLANTACIÓN
PR-4C	lun 04/07/16		1.0	Comisión Seguridad	Comisión Dirección
DURACION	4 semana	FECHA INICIO	29/07/16	PRESUPUESTO:	700 horas/hombre €

OBJETIVOS	Realización de auditoría de seguridad del paciente.
DESCRIPCION	Obtención de la los informes de mejora de las Tecnologías de la Información Sanitaria resultado de la aplicación de la metodología de las Guías SAFER.
BENEFICIOS	Reducción de Eventos Adversos en la Seguridad del Paciente. Disminución en la estancia media de hospitalización, disminución de la repetición de pruebas diagnósticas innecesarias, disminución de intervenciones quirúrgicas innecesarias. Incremento del porcentaje de tiempo de sistemas disponibles. Ahorro en horas/hombre en resolución de incidentes relacionados con la disponibilidad de los sistemas.
INDICADORES	• Informes de Auditoría SAFER.

RIESGO A MITIGAR	**Riesgo**	**Acción**	**Riesgo Actual**	**Riesgo Objetivo**
	Deficiencias en la organización	REDUCIR	MA	M
	Escapes de información	REDUCIR	MA	M
	Errores de los usuarios	REDUCIR	MA	M
	Errores del administrador	REDUCIR	MA	M
	Errores de monitorización (log)	REDUCIR	MA	M
	Errores de Configuración	REDUCIR	MA	M
	Introducción de información incorrecta	REDUCIR	MA	M
	Alteración de la información	REDUCIR	MA	M

19. ANEXO XII. Evolución del Cumplimiento de la Norma ISO/IEC 27002 de la Fase 1 a la Fase 5

19.1. Políticas de seguridad

Un documento denominado "política" es aquel que expresa una intención e instrucción global en la manera que formalmente ha sido expresada por la Dirección de la organización.

El contenido de las políticas se basa en el contexto en el que opera una organización y suelen ser considerados en su redacción los fines y objetivos de la organización, las estrategias adoptadas para alcanzar sus objetivos, la estructura y los procesos adoptados por la organización, los objetivos generales y específicos relacionados con el tema de la política y requisitos de las políticas procedentes de niveles más superiores (legales de obligado cumplimiento, del sector al que pertenece la organización, de la propia organización de niveles superiores o más ámplios, ...) relacionadas.

Dominio	Políticas de la Seguridad de la Información
Proyectos influyentes	PR-2A Planificación para la Prevención de incidentes
	PR-3A Planificación de la Continuidad del Negocio y Recuperación de Desastres
	PR-4A Creación de los mecanismos organizativos para la evaluación de las tecnologías de la información y la seguridad del paciente.
Controles Afectados	A.5.1.1, A.5.1.2

Tabla 36. Proyectos influyentes sobre el Dominio Políticas de la Seguridad de la Información

Control	Controles y objetivos de control	Efectividad Fase 5	Efectividad Fase 1
A.5	**POLÍTICAS DE SEGURIDAD**	**90%**	**10%**
A.5.1	**Directrices de la Dirección en seguridad de la información**	**90%**	**10%**
A.5.1.1	Conjunto de políticas para la seguridad de la información	90%	10%
A.5.1.2	Revisión de las políticas para la seguridad de la información	90%	10%

Tabla 37. Evolución de los Controles de Políticas de Segridad

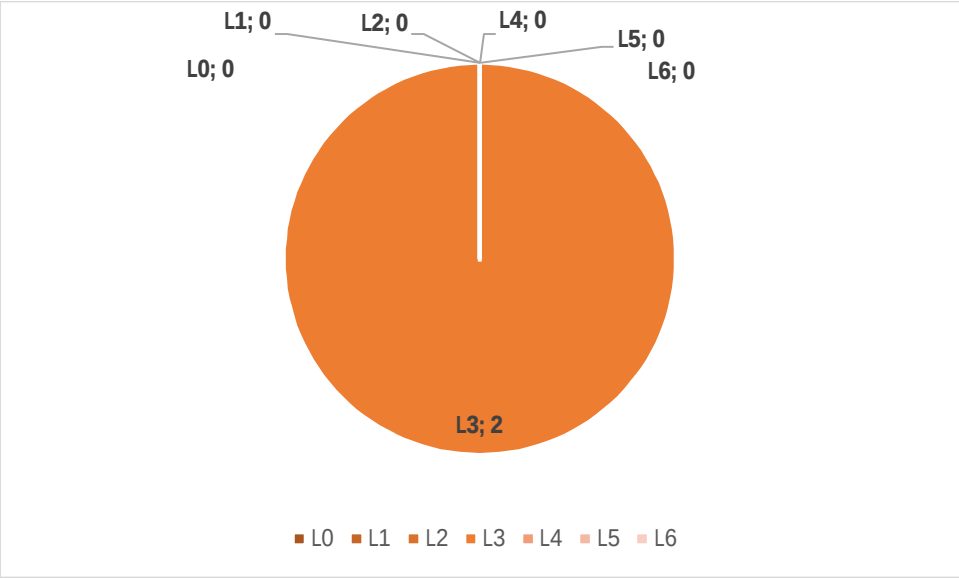


Ilustración 20. Controles por Niveles de Madurez Políticas de Seguridad

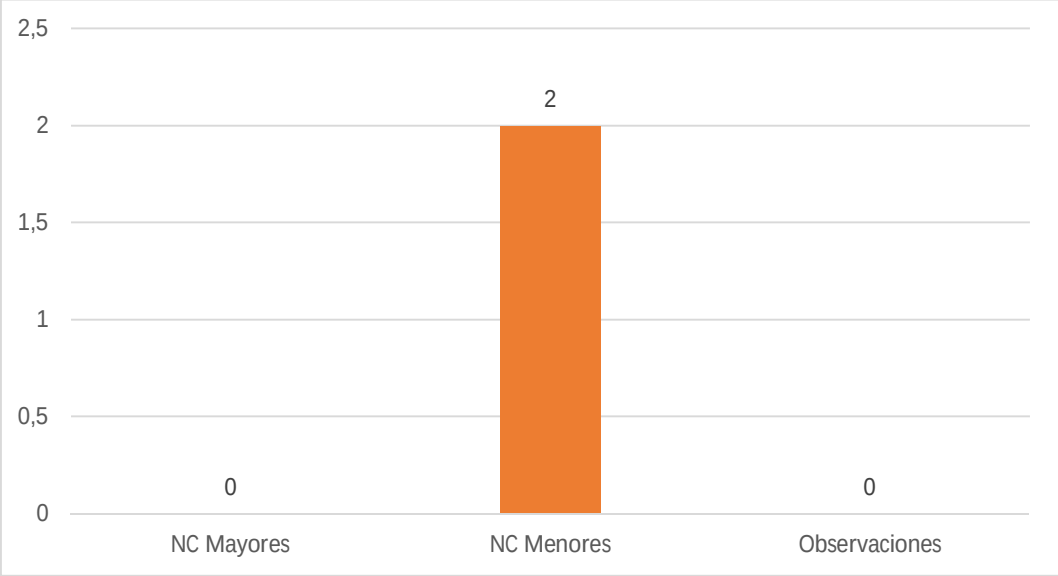


Ilustración 21. No conformidades Políticas de Seguridad

19.2. Aspectos organizativos de la seguridad de la información

El objetivo del presente dominio es establecer la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la organización.

Para ello se debería definir formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de las políticas de seguridad, la coordinación de la implementación de la seguridad y la asignación de funciones y responsabilidades.

Para una actualización adecuada en materia de seguridad se debería contemplar la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad de la información.

Las protecciones físicas de las organizaciones son cada vez más reducidas por las actividades de la organización requiere por parte del personal interno/externo que acceden a información

desde el exterior en situación de mobilidad temporal o permanente. En estos casos se considera que la información puede ponerse en riesgo si el acceso se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

Dominio	Aspectos organizativos de la seguridad de la información
Proyectos influyentes	PR-2A Planificación para la Prevención de incidentes
	PR-3A Planificación de la Continuidad del Negocio y Recuperación de Desastres
	PR-4A Creación de los mecanismos organizativos para la evaluación de las tecnologías de la información y la seguridad del paciente.
	PR-4B Plan de Auditoría de seguridad del paciente
Controles Afectados	A.6.1.2, A.6.1.1, A.6.1.4, A.6.1.5

Tabla 38. Proyectos influyentes sobre el Dominio Aspectos Organizativos de la Seguridad de la INformación

Control	Controles y objetivos de control	Efectividad Fase 5	Efectividad Fase 1
A.6	**Aspectos organizativos de la seguridad de la información**	**47%**	**29%**
A.6.1	**Organización interna**	**42%**	**6%**
A.6.1.1	Asignación de responsabilidades para la segur. de la información.	50%	10%
A.6.1.2	Segregación de tareas.	50%	0%
A.6.1.3	Contacto con las autoridades	10%	10%
A.6.1.4	Contacto con grupos de interés especial	50%	10%
A.6.1.5	Seguridad de la información en la gestión de proyectos	50%	0%
A.6.2	**Dispositivos para movilidad y teletrabajo.**	**53%**	**53%**
A.6.2.1	Política de uso de dispositivos para movilidad.	10%	10%
A.6.2.2	Teletrabajo.	95%	95%

Tabla 39. Evolución de los Controles de los Aspectos Organizativos de la Seguridad de la Información

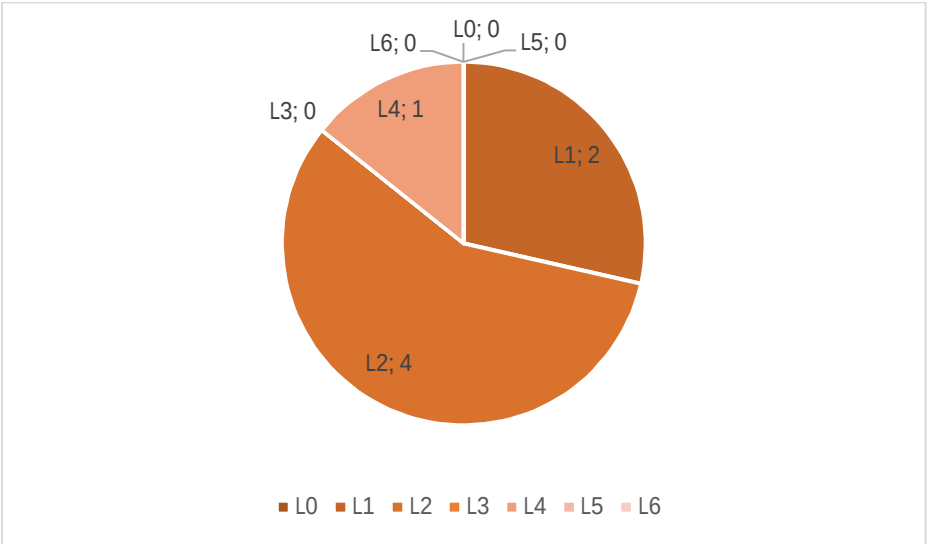


Ilustración 22. Controles por Niveles de Madurez Aspectos Organizativos de la Seguridad de la Información

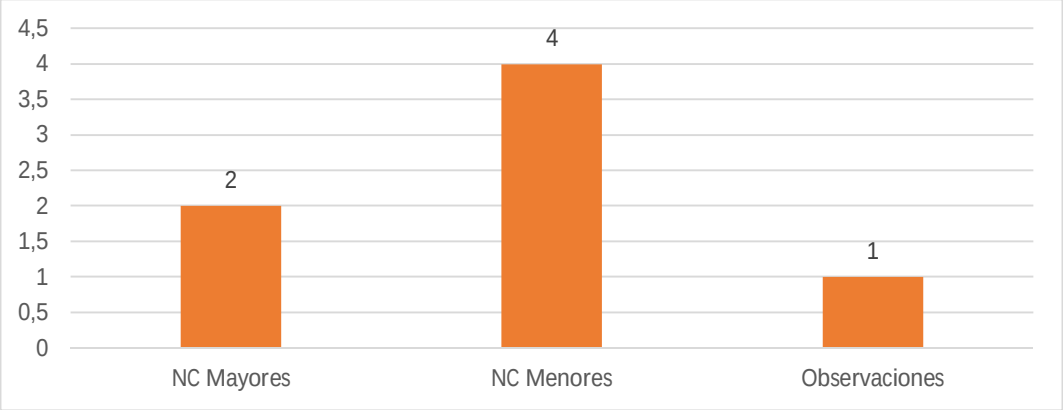


Ilustración 23. No conformidades Aspectos Organizativos de la Seguridad de la Información

19.3. Seguridad ligada a los recursos humanos

El objetivo del presente dominio es la necesidad de educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.

Es necesario reducir los riesgos de error humano, comisión de actos ilícitos, uso inadecuado de instalaciones y recursos y manejo no autorizado de la información, junto a la definición de posibles sanciones que se aplicarán en caso de incumplimiento.

Dominio	Seguridad ligada a los recursos humanos
Proyectos influyentes	PR-1A a. Concienciación a usuarios y profesionales TIC
Controles Afectados	A.7.2.1, A.7.2.2

Tabla 40. Proyectos influyentes sobre el Dominio Seguridad Ligada a los Recursos Humanos

Control	Controles y objetivos de control	Efectividad Fase 5	Efectividad Fase 1
A.7	**Seguridad ligada a los recursos humanos**	**61%**	**42%**
A.7.1	**Antes de la Contratación**	**92%**	**63%**
A.7.1.1	Investigación de antecedentes.	N/A	N/A
A.7.1.2	Términos y condiciones de contratación.	95%	95%
A.7.2	**Durante la contratación.**	**92%**	**63%**
A.7.2.1	Responsabilidades de gestión.	90%	10%
A.7.2.2	Concienciación, educación y capacitación en segur. de la informac.	95%	90%
A.7.2.3	Proceso disciplinario.	90%	90%
A.7.3	**Cese o cambio de puesto de trabajo.**	**0%**	**0%**
A.7.3.1	Cese o cambio de puesto de trabajo.	0%	0%

Tabla 41. Evolución de los Controles de la Seguridad Ligada a los Recursos Humanos

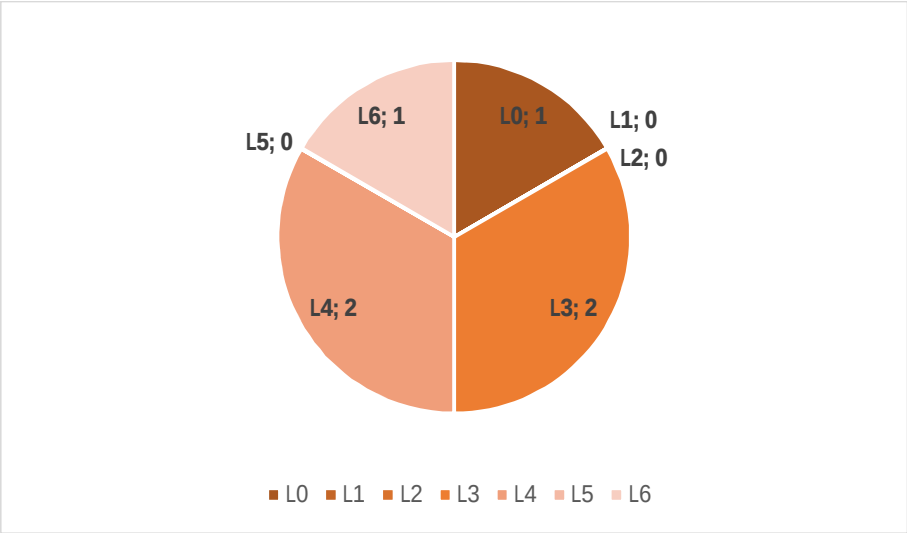


Ilustración 24. Controles por Niveles de Madurez Seguridad LIgada a los Recursos Humanos

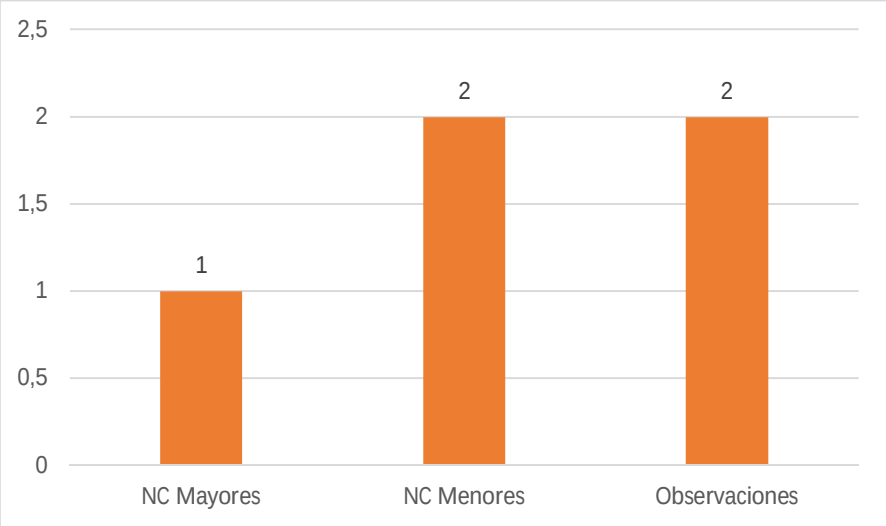


Ilustración 25. No conformidades Seguridad Ligada a los Recursos Humanos

19.4. Gestión de activos

El objetivo del presente dominio es que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos.

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Dominio	Gestión de activos
Proyectos influyentes	Ninguno
Controles Afectados	Ninguno

Tabla 42. Proyectos influyentes sobre el Dominio Gestión de Activos

Control	Controles y objetivos de control	Efectividad Fase 5	Efectividad Fase 1
A.8	**GESTIÓN DE ACTIVOS.**	**15%**	**15%**
A.8.1	**Responsabilidad sobre los activos.**	**28%**	**28%**
A.8.1.1	Inventario de activos.	10%	10%
A.8.1.2	Propiedad de los activos.	10%	10%
A.8.1.3	Uso aceptable de los activos.	90%	90%
A.8.1.4	Devolución de activos.	-	-
A.8.2	**Clasificación de la información.**	**10%**	**10%**
A.8.2.1	Directrices de clasificación.	10%	10%
A.8.2.2	Etiquetado y manipulado de la información.	10%	10%
A.8.2.3	Manipulación de activos.	10%	10%
A.8.3	**Manejo de los soportes de almacenamiento.**	**7%**	**7%**
A.8.3.1	Gestión de soportes extraíbles.	10%	10%
A.8.3.2	Eliminación de soportes.	10%	10%
A.8.3.3	Soportes físicos en tránsito	-	-

Tabla 43. Evolución de los Controles de la Gestión de Activos

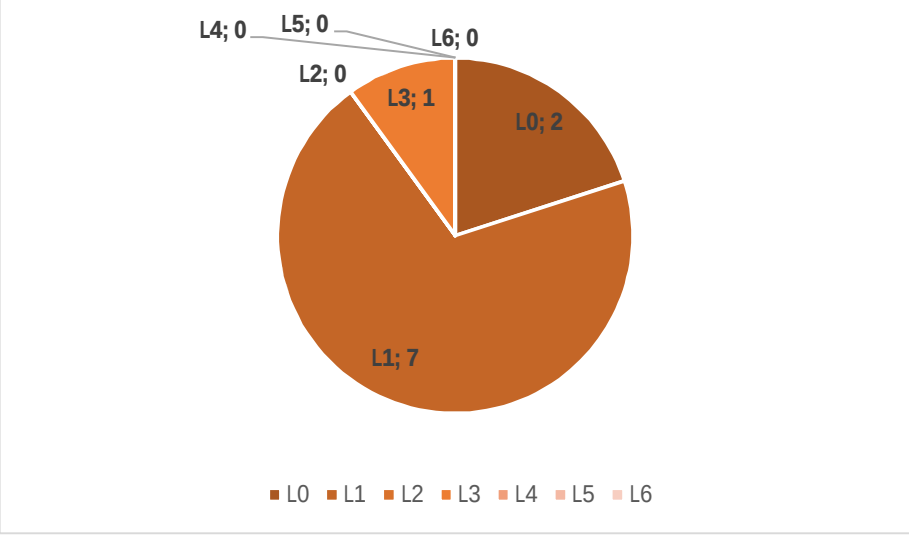


Ilustración 26. Controles por Niveles de Madurez Gestión de Activos

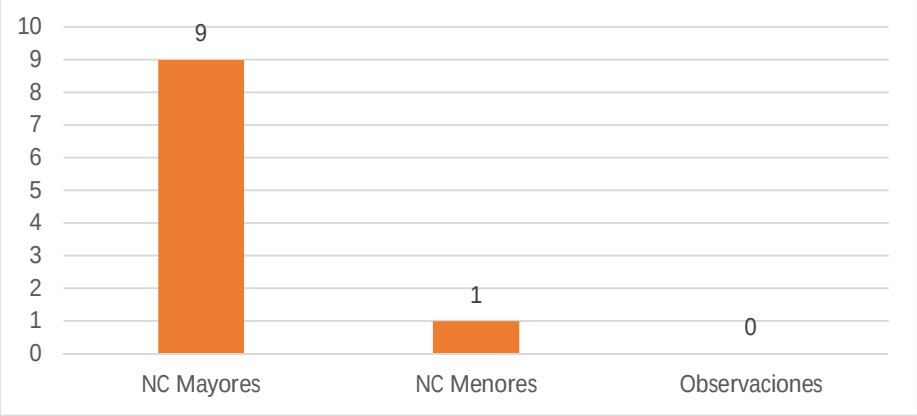


Ilustración 27. No conformidades Gestión de Activos

19.5. Control de accesos

El objetivo del presente dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.

Para impedir el acceso no autorizado a los sistemas de información se deberían implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Dominio	Control de accesos
Proyectos influyentes	Ninguno
Controles Afectados	Ninguno

Tabla 44. Proyectos influyentes sobre el Dominio Control de Accesos

Control	Controles y objetivos de control	Efectividad Fase 5	Efectividad Fase 1
A.9	**Control de accesos**	**8%**	**8%**
A.9.1	**Requisitos de negocio para el control de accesos.**	**10%**	**10%**
A.9.1.1	Política de control de accesos.	10%	10%
A.9.1.2	Control de acceso a las redes y servicios asociados.	10%	10%
A.9.2	**Gestión de acceso de usuario.**	**3%**	**3%**
A.9.2.1	Gestión de altas/bajas en el registro de usuarios.	10%	10%
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios.	10%	10%
A.9.2.3	Gestión de los derechos de acceso con privilegios especiales.	0%	0%
A.9.2.4	Gestión de información confidencial de autenticación de usuarios.	0%	0%
A.9.2.5	Revisión de los derechos de acceso de los usuarios.	0%	0%
A.9.2.6	Retirada o adaptación de los derechos de acceso	0%	0%
A.9.3	**Responsabilidades del usuario.**	**10%**	**10%**
A.9.3.1	Uso de información confidencial para la autenticación.	10%	10%
A.9.4	**Control de acceso a sistemas y aplicaciones.**	**10%**	**10%**
A.9.4.1	Restricción del acceso a la información.	10%	10%
A.9.4.2	Procedimientos seguros de inicio de sesión.	10%	10%
A.9.4.3	Gestión de contraseñas de usuario.	10%	10%
A.9.4.4	Uso de herramientas de administración de sistemas.	10%	10%
A.9.4.5	Control de acceso al código fuente de los programas.	10%	10%

Tabla 45. Evolución de los Controles de Control de Accesos

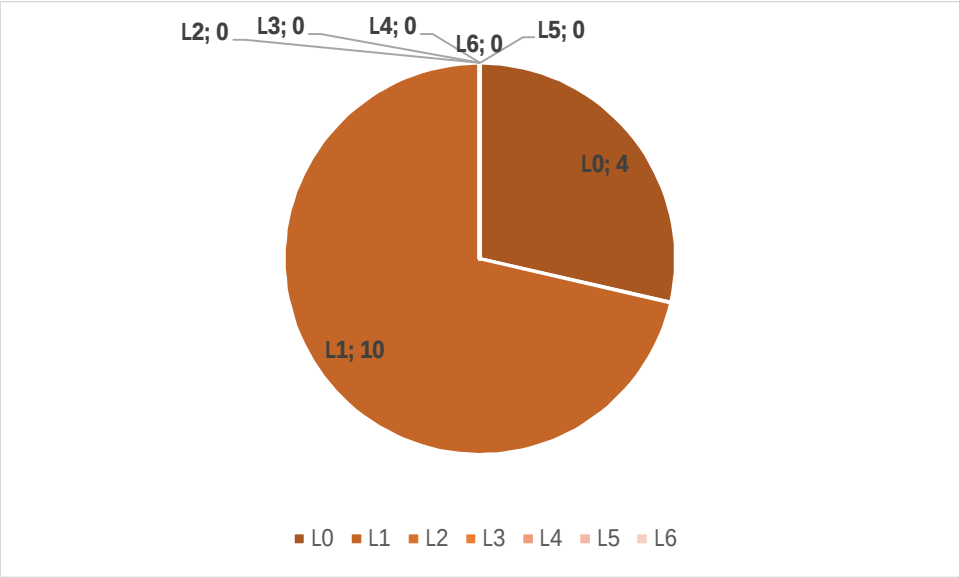


Ilustración 28. Controles por Niveles de Madurez Control de Accesos

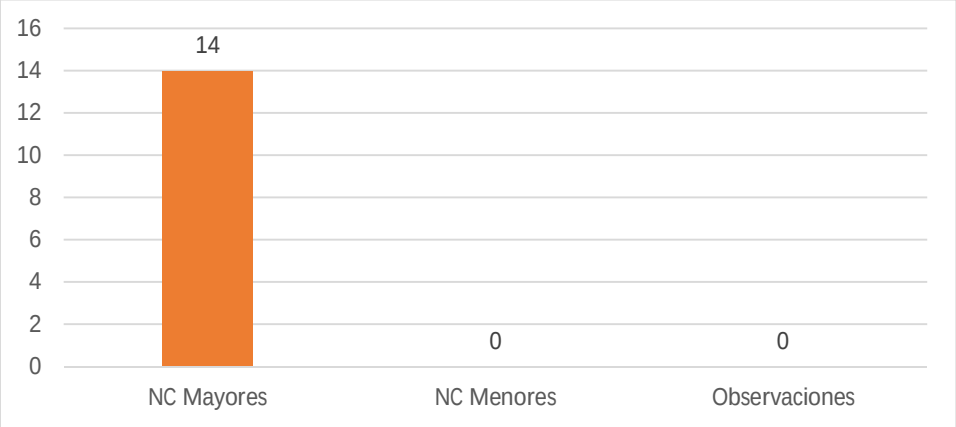


Ilustración 29. No conformidades Control de Accesos

19.6. Cifrado

El objetivo del presente dominio es el uso de sistemas y técnicas criptográficas para la protección de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

La aplicación de medidas de cifrado se debería desarrollar en base a una política sobre el uso de controles criptográficos y al establecimiento de una gestión de las claves que sustenta la aplicación de las técnicas criptográficas.

Dominio	Cifrado
Proyectos influyentes	Ninguno
Controles Afectados	Ninguno

Tabla 46. Proyectos influyentes sobre el Dominio Cifrado

Control	Controles y objetivos de control	Efectividad Fase 5	Efectividad Fase 1
A.10	**Cifrado**	**10%**	**10%**
A.10.1	**Controles criptográficos.**	**10%**	**10%**
A.10.1.1	Política de uso de los controles criptográficos.	10%	10%
A.10.1.2	Gestión de claves.	10%	10%

Tabla 47. Evolución de los Controles de Cifrado

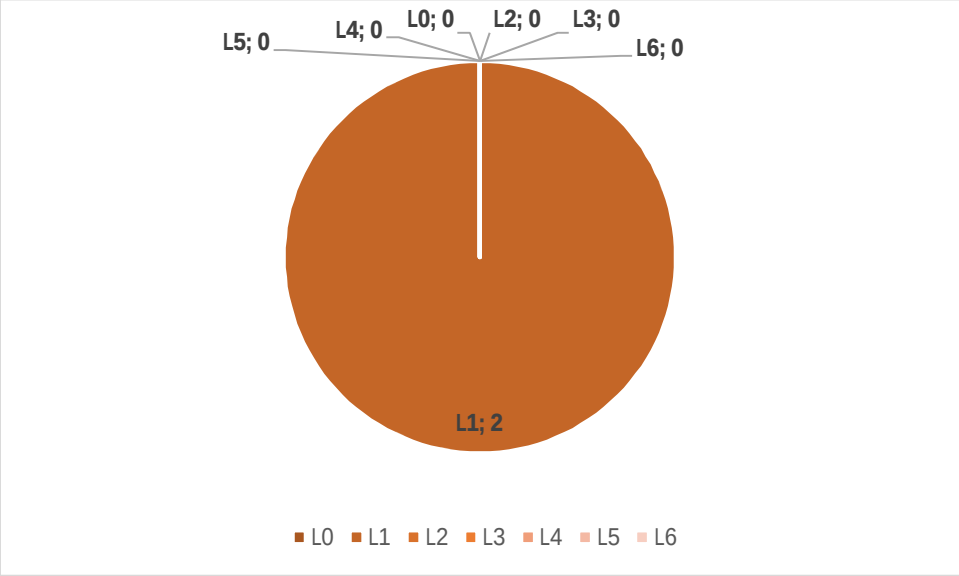


Ilustración 30. Controles por Niveles de Madurez Cifrado

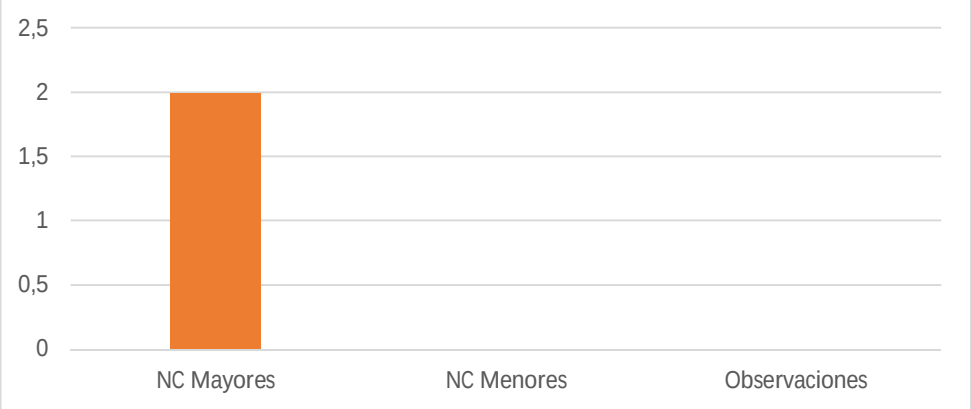


Ilustración 31. No conformidades Cifrado

19.7. Seguridad física y ambiental

El objetivo es minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección de las instalaciones de procesamiento de información crítica o sensible de la organización, contra accesos físicos no autorizados.

El control de los factores ambientales de origen interno y/o externo permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados, especialmente en casos en los que el equipamiento perteneciente a la organización estén físicamente fuera del mismo (housing) o en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información (hosting/cloud).

Dominio	**Seguridad física y ambiental**
Proyectos influyentes	Ninguno
Controles Afectados	Ninguno

Tabla 48. Proyectos influyentes sobre el Dominio Seguridad Física y Ambiental

Control	Controles y objetivos de control	Efectividad Fase 5	Efectividad Fase 1
A.11	**Seguridad física y ambiental**	**31%**	**31%**
A.11.1	**Áreas seguras.**	**23%**	**23%**
A.11.1.1	Perímetro de seguridad física.	10%	10%
A.11.1.2	Controles físicos de entrada.	10%	10%
A.11.1.3	Seguridad de oficinas, despachos y recursos.	10%	10%
A.11.1.4	Protección contra las amenazas externas y ambientales.	50%	50%
A.11.1.5	El trabajo en áreas seguras.	10%	10%
A.11.1.6	Áreas de acceso público, carga y descarga.	50%	50%
A.11.2	**Seguridad de los equipos.**	**39%**	**39%**
A.11.2.1	Emplazamiento y protección de equipos.	50%	50%
A.11.2.2	Instalaciones de suministro.	90%	90%
A.11.2.3	Seguridad del cableado.	10%	10%
A.11.2.4	Mantenimiento de los equipos.	50%	50%
A.11.2.5	Salida de activos fuera de las dependencias de la empresa.	0%	0%
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	0%	0%
A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	50%	50%
A.11.2.8	Equipo informático de usuario desatendido.	50%	50%
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	50%	50%

Tabla 49. Evolución de los Controles de Seguridad Física y Ambiental

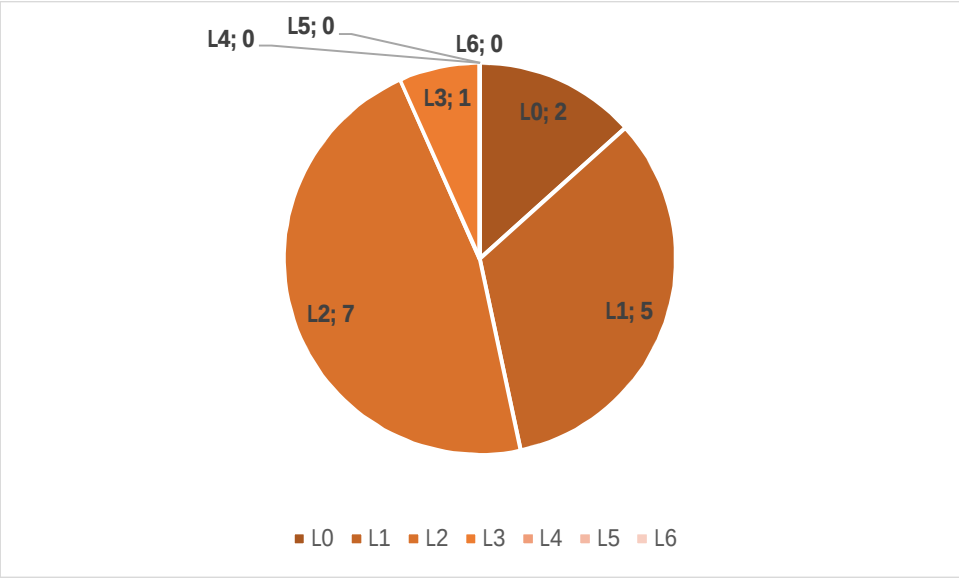


Ilustración 32. Controles por Niveles Seguridad Física y Ambiental

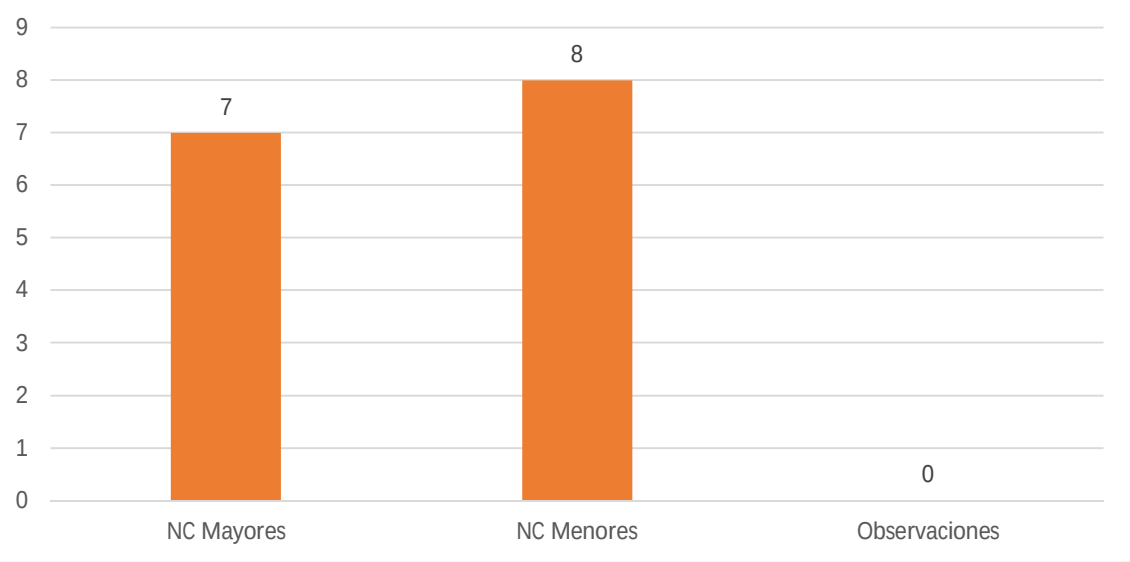


Ilustración 33. No conformidades Seguridad Física y Ambiental

19.8. Seguridad en la operativa

El objetivo es controlar la existencia de los procedimientos de operaciones y el desarrollo y mantenimiento de documentación actualizada relacionada.

Adicionalmente, se debería evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando las responsabilidades correspondientes y administrando los medios técnicos necesarios para permitir la segregación de los ambientes y responsabilidades en el procesamiento.

Con el fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario, sería necesario monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad.

Dominio	Seguridad en la operativa
Proyectos influyentes	PR-1E Formación a usuarios y profesionales TIC en Seguridad del Paciente
	PR-2E Implantación de sistemas IDS/IPS
	PR-3B Implantación y Operación plan para la continuidad del negocio y recuperación de desastres
	PR-4B Plan de Auditoría de seguridad del paciente
Controles Afectados	A.12.2.1, A.12.3.1 A.12.4.1, A.12.4.2, A.12.4.3, A.12.7.1, A.12.1.4

Tabla 50. Proyectos influyentes sobre el Dominio Seguridad en la Operativa

Control	Controles y objetivos de control	Efectividad Fase 5	Efectividad Fase 1
A.12	**Seguridad en la operativa**	**53%**	**8%**
A.12.1	**Responsabilidades y procedimientos de operación.**	**8%**	**8%**
A.12.1.1	Documentación de procedimientos de operación.	10%	10%
A.12.1.2	Gestión de cambios.	0%	0%
A.12.1.3	Gestión de capacidades.	10%	10%
A.12.1.4	Separación de entornos de desarrollo, prueba y producción.	10%	10%
A.12.2	**Protección contra código malicioso.**	**90%**	**10%**
A.12.2.1	Controles contra el código malicioso.	90%	10%
A.12.3	**Copias de seguridad.**	**90%**	**10%**
A.12.3.1	Copias de seguridad de la información.	90%	10%
A.12.4	**Registro de actividad y supervisión.**	**70%**	**5%**
A.12.4.1	Registro y gestión de eventos de actividad.	90%	0%
A.12.4.2	Protección de los registros de información.	90%	10%
A.12.4.3	Registros de actividad del administrador y operador del sistema.	90%	0%
A.12.4.4	Sincronización de relojes.	10%	10%
A.12.5	**Control del software en explotación.**	**10%**	**10%**
A.12.5.1	Instalación del software en sistemas en producción.	10%	10%
A.12.6	**Gestión de la vulnerabilidad técnica.**	**10%**	**10%**
A.12.6.1	Gestión de las vulnerabilidades técnicas.	10%	10%
A.12.6.2	Restricciones en la instalación de software.	10%	10%
A.12.7	**Consideraciones de las auditorías de los sistemas de información.**	**90%**	**0%**
A.12.7.1	Controles de auditoría de los sistemas de información.	90%	0%

Tabla 51. Evolución de los Controles de la Seguridad Operativa

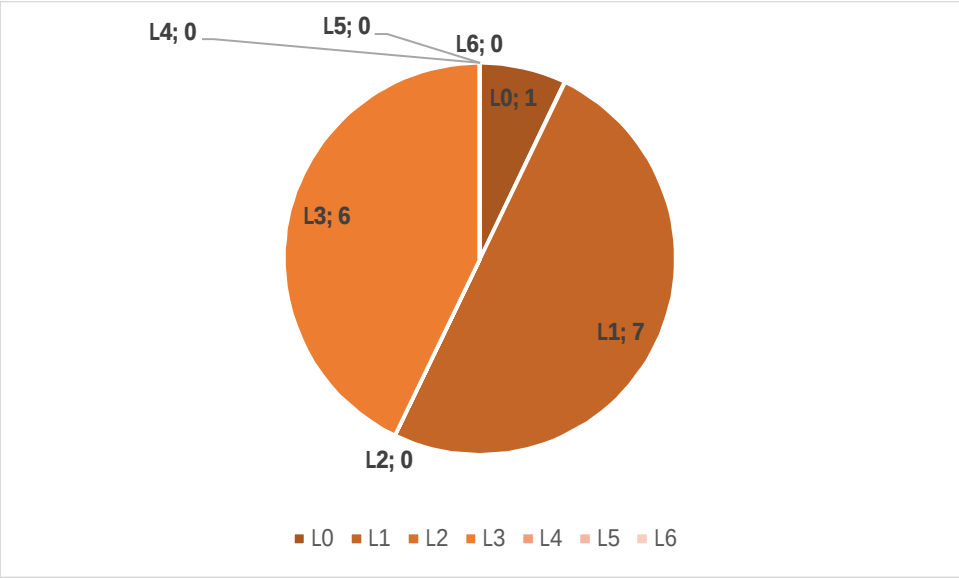


Ilustración 34. Controles por Niveles Seguridad Operativa

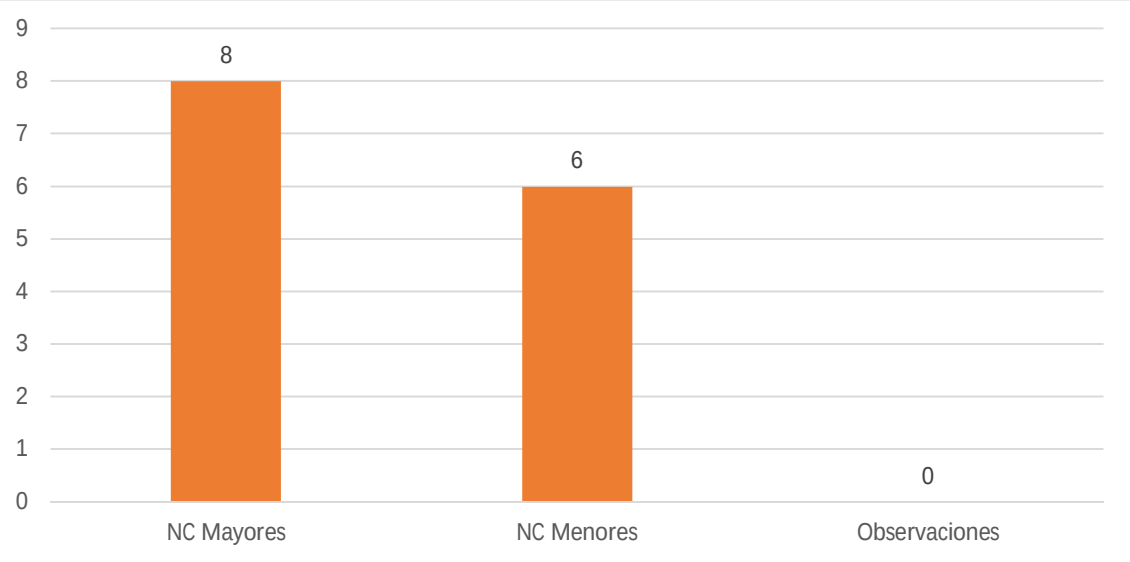


Ilustración 35. No conformidades Seguridad en la Operativa

19.9. Seguridad en las telecomunicaciones

El objetivo es asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte.

La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección.

Dominio	Seguridad en las telecomunicaciones
Proyectos influyentes	Ninguno
Controles Afectados	Ninguno

Tabla 52. Proyectos influyentes sobre el Dominio Seguridad en las Telecomunicaciones

Control	Controles y objetivos de control	Efectividad Fase 5	Efectividad Fase 1
A.13	**Seguridad en las telecomunicaciones**	**23%**	**23%**
A.13.1	**Gestión de la seguridad en las redes.**	**37%**	**37%**
A.13.1.1	Controles de red.	50%	50%
A.13.1.2	Mecanismos de seguridad asociados a servicios en red.	50%	50%
A.13.1.3	Segregación de redes.	10%	10%
A.13.2	**Intercambio de información con partes externas.**	**10%**	**10%**
A.13.2.1	Políticas y procedimientos de intercambio de información.	10%	10%
A.13.2.2	Acuerdos de intercambio.	10%	10%
A.13.2.3	Mensajería electrónica.	10%	10%
A.13.2.4	Acuerdos de confidencialidad y secreto.	10%	10%

Tabla 53. Evolución de los Controles de la Seguridad en las Telecomunicacones

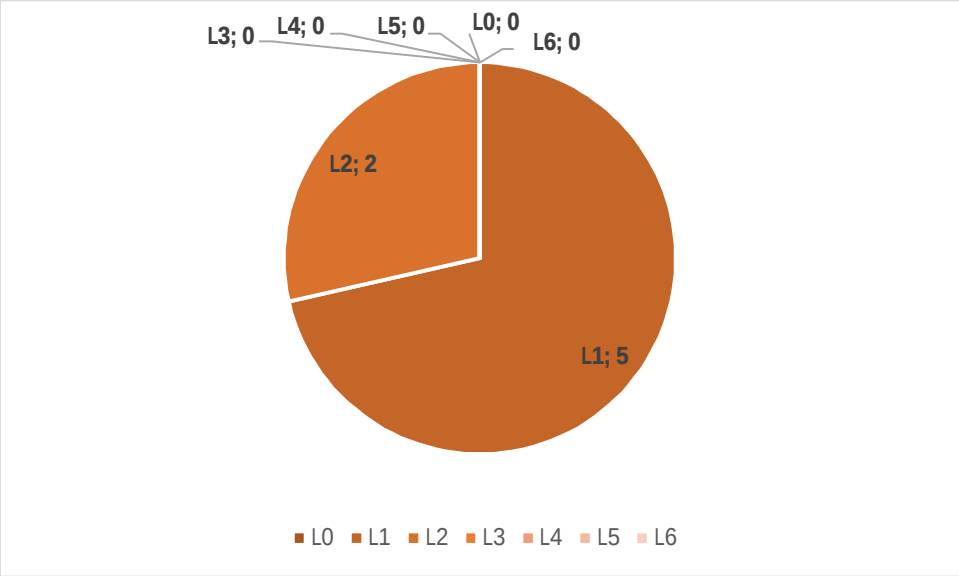


Ilustración 36. Controles por Niveles Seguridad en las Telecomunicaciones

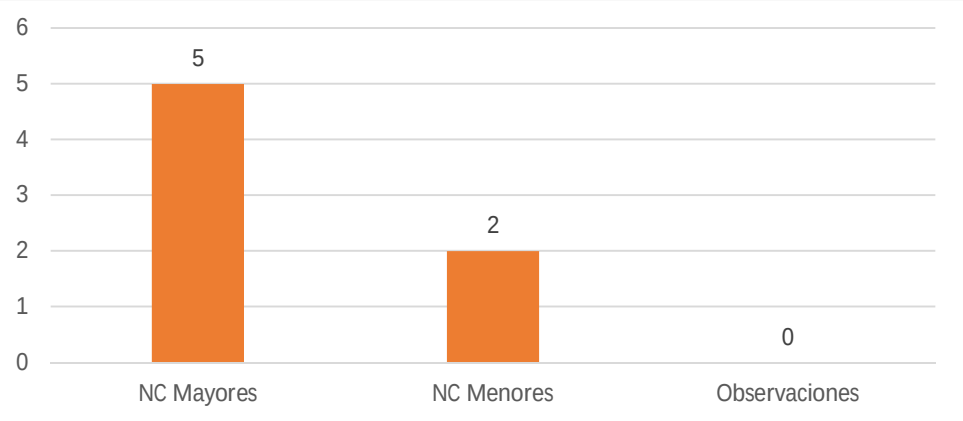


Ilustración 37. No conformidades Seguridad en las Telecomunicaciones

19.10. Adquisición, desarrollo y mantenimiento de los sistemas de información.

El objetivo es asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información.

Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

Definir los métodos de protección de la información crítica o sensible.

Aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software que integren cualquiera de los ambientes administrados por la organización en donde residan los desarrollos mencionados.

Dominio	Adquisición, desarrollo y mantenimiento de los sistemas de información
Proyectos influyentes	PR-4B Plan de Auditoría de seguridad del paciente
Controles Afectados	A.14.1.1, A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9, A.14.3.1

Tabla 54. Proyectos influyentes sobre el Dominio Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

Control	Controles y objetivos de control	Efectividad Fase 5	Efectividad Fase 1
A.14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**	**70%**	**12%**
A.14.1	**Requisitos de seguridad de los sistemas de información.**	**50%**	**20%**
A.14.1.1	Análisis y especificación de los requisitos de seguridad.	90%	0%
A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.	10%	10%
A.14.1.3	Protección de las transacciones por redes telemáticas.	50%	50%
A.14.2	**Seguridad en los procesos de desarrollo y soporte.**	**71%**	**7%**
A.14.2.1	Política de desarrollo seguro de software.	90%	0%
A.14.2.2	Procedimientos de control de cambios en los sistemas.	90%	10%
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	90%	0%
A.14.2.4	Restricciones a los cambios en los paquetes de software.	10%	10%
A.14.2.5	Uso de principios de ingeniería en protección de sistemas.	0%	0%
A.14.2.6	Seguridad en entornos de desarrollo.	90%	10%
A.14.2.7	Externalización del desarrollo de software.	90%	10%
A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	90%	10%
A.14.2.9	Pruebas de aceptación.	90%	10%
A.14.3	**Datos de prueba.**	**90%**	**10%**
A.14.3.1	Protección de los datos utilizados en pruebas.	90%	10%

Tabla 55. Evolución de los Controles de Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

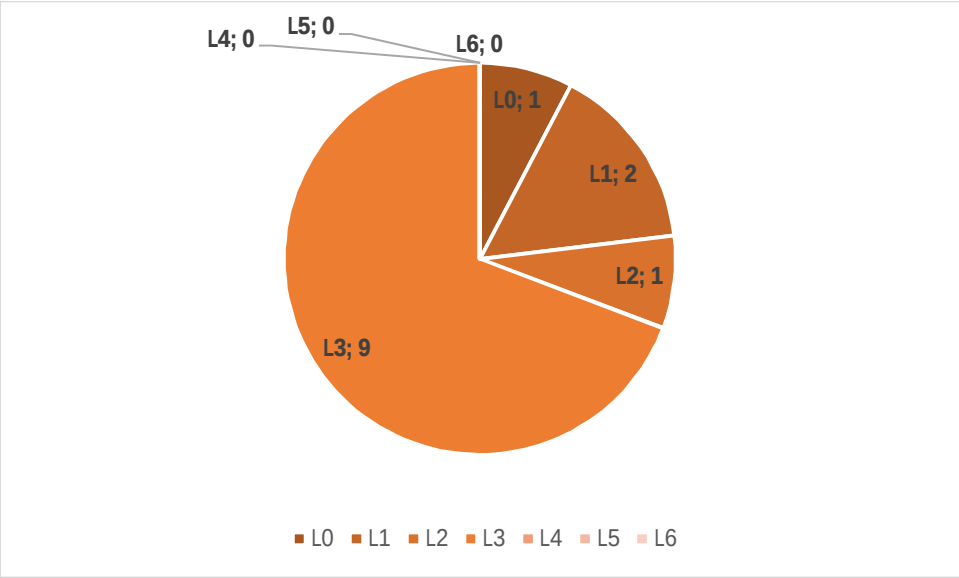


Ilustración 38. Controles por Niveles Seguridad Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

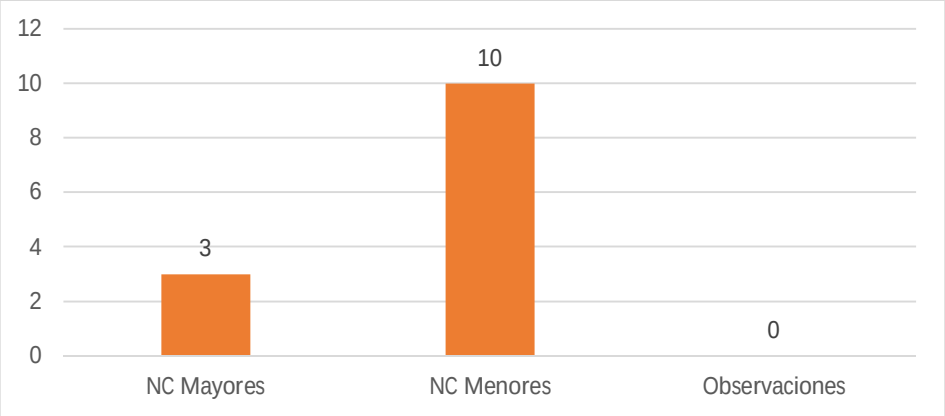


Ilustración 39. No Cumplimiento Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

19.11. Relaciones con suministradores

El objetivo es implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea con los acuerdos de entrega de servicios de terceros.

La organización debe chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados con terceras personas.

Dominio	Relaciones con suministradores
Proyectos influyentes	Ninguno
Controles Afectados	Ninguno

Tabla 56. Proyectos influyentes sobre el Dominio Relación con Suministradores

Control	Controles y objetivos de control	Efectividad Fase 5	Efectividad Fase 1
A.15	**Relaciones con suministradores**	**4%**	**4%**
A.15.1	**Seguridad de la información en las relaciones con suministradores.**	**3%**	**3%**
A.15.1.1	Política de seguridad de la información para suministradores.	10%	10%
A.15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.	0%	0%
A.15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.	0%	0%
A.15.2	**Gestión de la prestación del servicio por suministradores.**	**5%**	**5%**
A.15.2.1	Supervisión y revisión de los servicios prestados por terceros.	10%	10%
A.15.2.2	Gestión de cambios en los servicios prestados por terceros.	0%	0%

Tabla 57. Evolución de los Controles de Relaciones con Suministradores

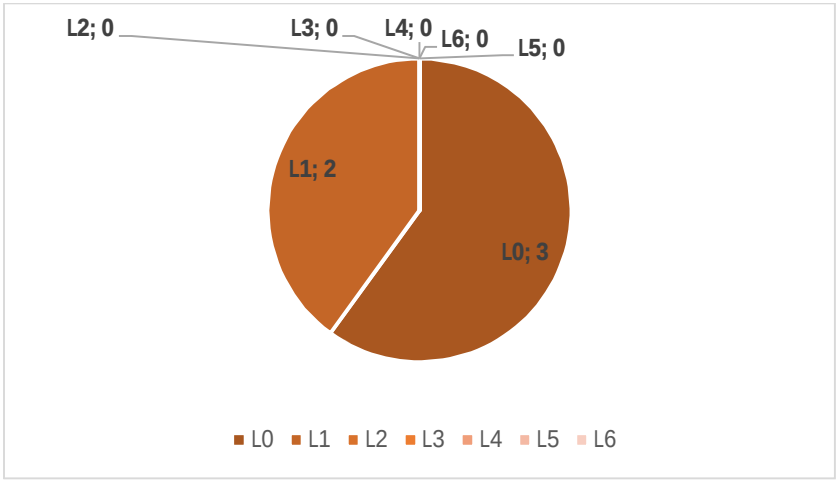


Ilustración 40. Controles por Niveles Seguridad Relaciones con Suministradores

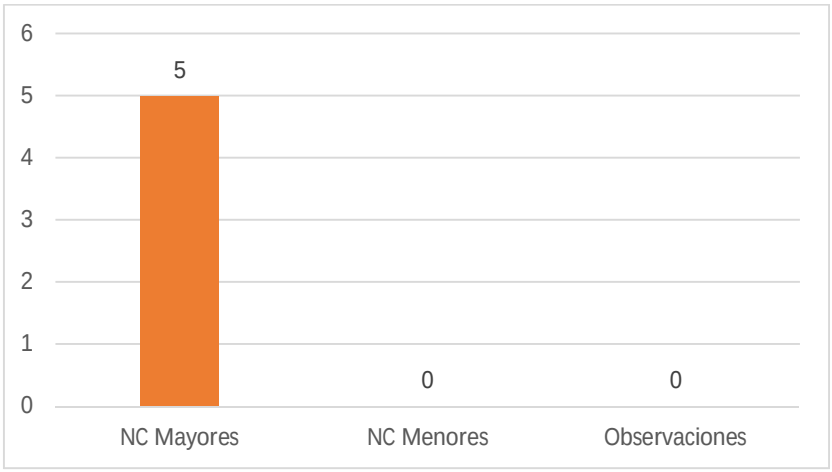


Ilustración 41. No Cumplimiento Relaciones con Suministradores

19.12. Gestión de incidentes en la seguridad de la información

El objetivo es garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.

Las organizaciones cuentan con innumerables activos de información, cada uno expuesto a sufrir incidentes de seguridad. Resulta necesario contar con una capacidad de gestión de dichos incidentes que permita comenzar por su detección, llevar a cabo su tratamiento y colaborar en la prevención de futuros incidentes similares.

Dominio	Gestión de incidentes en la seguridad de la información
Proyectos influyentes	PR-1B Formación a profesionales TIC (buenas prácticas, estándares, gestión de sistemas IDS/IPS)
	PR-1C Formación a profesionales TIC sobre las metodologías para la gestión de incidentes
	PR-1E Formación a usuarios y profesionales TIC en Seguridad del Paciente
	PR-1F Plan de difusión de sistemas de notificación de incidentes entre los usuarios
	PR-2A Planificación para la Prevención de incidentes
	PR-2B Planificación para la Detección y Análisis de incidentes
	PR-2C Planificación para la Contención de incidentes
	PR-2D Planificación para la Resolución de incidentes
	PR-2E Implantación de sistemas IDS/IPS
Controles Afectados	A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7

Tabla 58. Proyectos influyentes sobre el Dominio Gestióhn de Incidentes en la Seguridad de la Información

Control	Controles y objetivos de control	Efectividad Fase 5	Efectividad Fase 1
A.16	**Gestión de incidentes en la seguridad de la información**	**90%**	**1%**
A.16.1	**Gestión de incidentes de seguridad de la información y mejoras.**	**90%**	**1%**
A.16.1.1	Responsabilidades y procedimientos.	90%	10%
A.16.1.2	Notificación de los eventos de seguridad de la información.	90%	0%
A.16.1.3	Notificación de puntos débiles de la seguridad	90%	0%
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.	90%	0%
A.16.1.5	Respuesta a los incidentes de seguridad.	90%	0%
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información.	90%	0%
A.16.1.7	Recopilación de evidencias.	90%	0%

Tabla 59. Evolución de los Controles de la Gestión de Incidetes de Seguridad de la Información

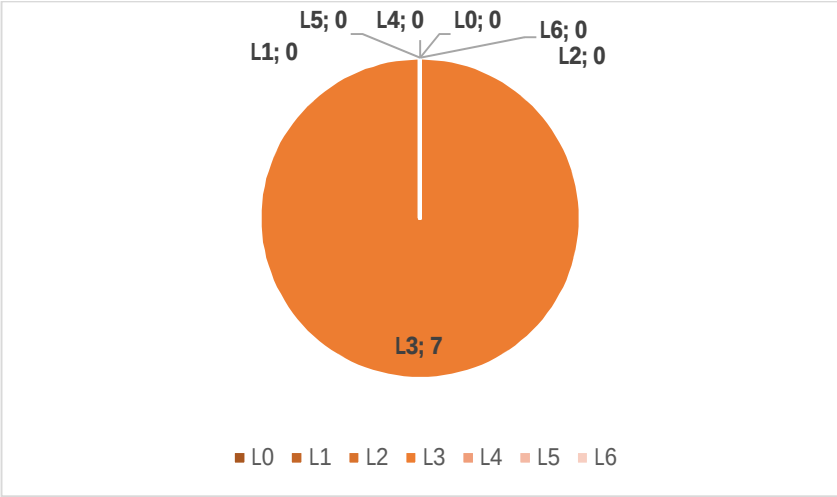


Ilustración 42. Controles por Niveles Seguridad Gestión de Incidentes en la Seguridad de la Información

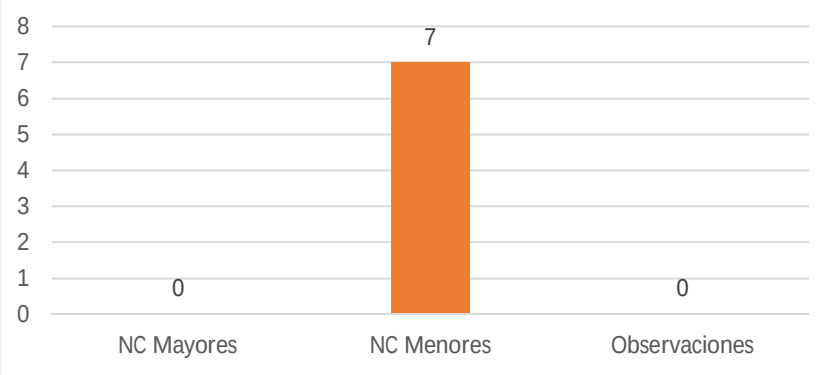


Ilustración 43. No Cumplimiento Gestión de Incidentes en la Seguridad de la Información

19.13. Aspectos de seguridad de la informacion en la gestión de la continuidad del negocio

El objetivo es preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad.

Se debería integrar dentro de los procesos críticos de negocio, aquellos requisitos de gestión de la seguridad de la información con atención especial a la legislación, las operaciones, el personal, los materiales, el transporte, los servicios y las instalaciones adicionales, alternativos y/o que estén dispuestos de un modo distinto a la operativa habitual.

Dominio	Aspectos de seguridad de la informacion en la gestión de la continuidad del negocio
Proyectos influyentes	PR-1D Formación a profesionales TIC sobre las metodologías para la continuidad del negocio y la recuperación de desastres
	PR-2D Planificación para la Resolución de incidentes
	PR-3A Planificación de la Continuidad del Negocio y Recuperación de Desastres
	PR-3B Implantación y Operación plan para la continuidad del negocio y recuperación de desastres
	PR-3C Auditoría de Seguridad del Paciente
Controles Afectados	A.17.1.1, A.17.1.2, A.17.1.3, A.17.2.1

Tabla 60. Proyectos influyentes sobre el Dominio Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio

Control	Controles y objetivos de control	Efectividad Fase 5	Efectividad Fase 1
A.17	**Aspectos de seguridad de la informacion en la gestión de la continuidad del negocio**	**90%**	**5%**
A.17.1	**Continuidad de la seguridad de la información.**	**90%**	**0%**
A.17.1.1	Planificación de la continuidad de la seguridad de la información.	90%	0%
A.17.1.2	Implantación de la continuidad de la seguridad de la información.	90%	0%
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la Seguridad de la información.	90%	0%
A.17.2	**Redundancias.**	**90%**	**10%**
A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	90%	10%

Tabla 61. Evolución de los Controles de los Aspectos de Seguridad de la Información de la Continuidad del Negocio

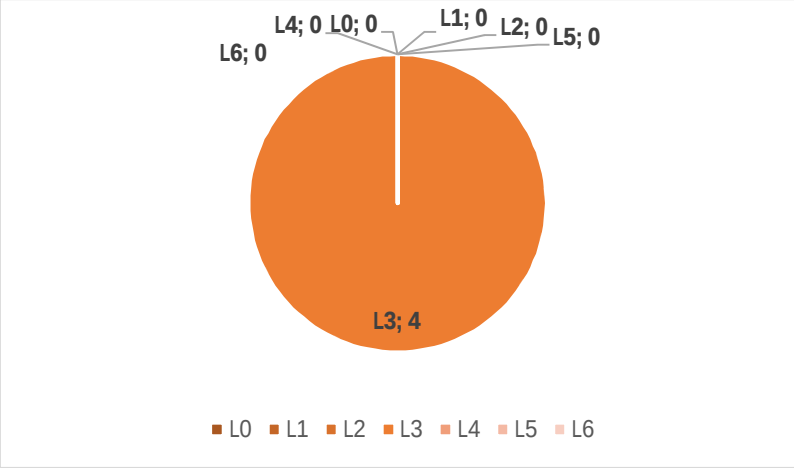


Ilustración 44. Controles por Niveles Seguridad Gestión de la Continuidad del Negocio

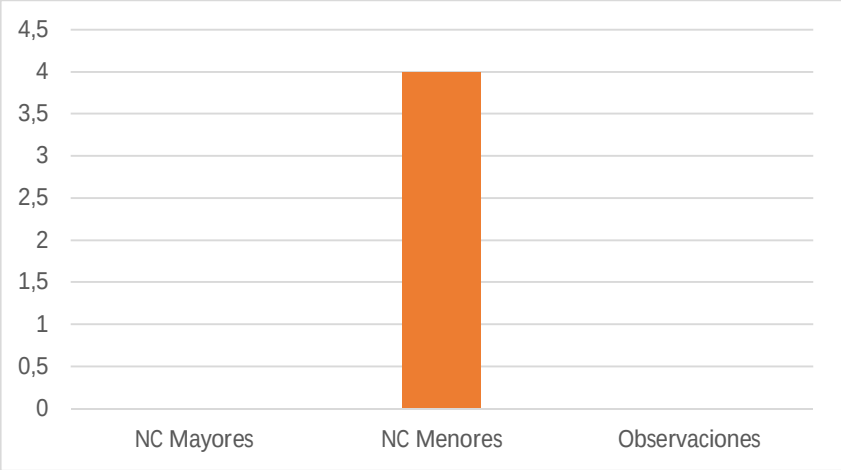


Ilustración 45. No Cumplimiento Gestión de la Continuidad del Negocio

19.14. Cumplimiento

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.

Los requisitos normativos y contractuales pertinentes a cada sistema de información deberían estar debidamente definidos y documentados.

El objetivo es cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la organización y/o a los empleados que incurran en responsabilidad civil o penal como resultado de incumplimientos.

Se debe revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

Dominio	Cumplimiento
Proyectos influyentes	PR-1A Concienciación a usuarios y profesionales TIC
	PR-4B Plan de Auditoría de seguridad del paciente
Controles Afectados	A.18.1, A.18.2

Tabla 62. Proyectos influyentes sobre el Dominio Cumplimiento Legal

Control	Controles y objetivos de control	Efectividad Fase 5	Efectividad Fase 1
A.18	**Cumplimiento**	**81%**	**25%**
A.18.1	**Cumplimiento de los requisitos legales y contractuales.**	**72%**	**40%**
A.18.1.1	Identificación de la legislación aplicable.	90%	50%
A.18.1.2	Derechos de propiedad intelectual (DPI).	90%	50%
A.18.1.3	Protección de los registros de la organización.	90%	50%
A.18.1.4	Protección de datos y privacidad de la información personal.	90%	50%
A.18.1.5	Regulación de los controles criptográficos.	0%	0%
A.18.2	**Revisiones de la seguridad de la información.**	**90%**	**10%**
A.18.2.1	Revisión independiente de la seguridad de la información.	90%	10%
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	90%	10%
A.18.2.3	Comprobación del cumplimiento	90%	10%

Tabla 63. Evolución de los Controles de Cumplimiento Legal

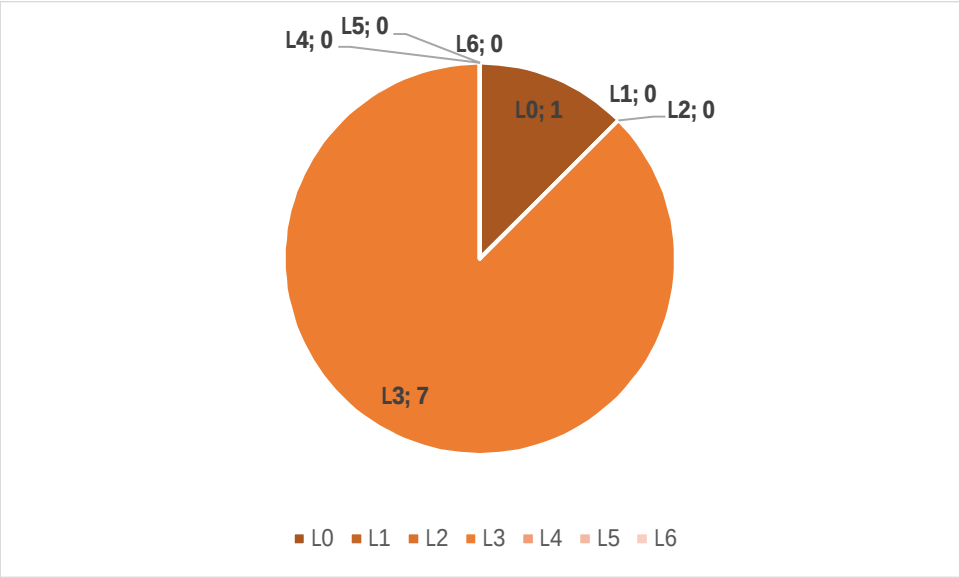


Ilustración 46. Controles por Niveles Cumplimiento Legal

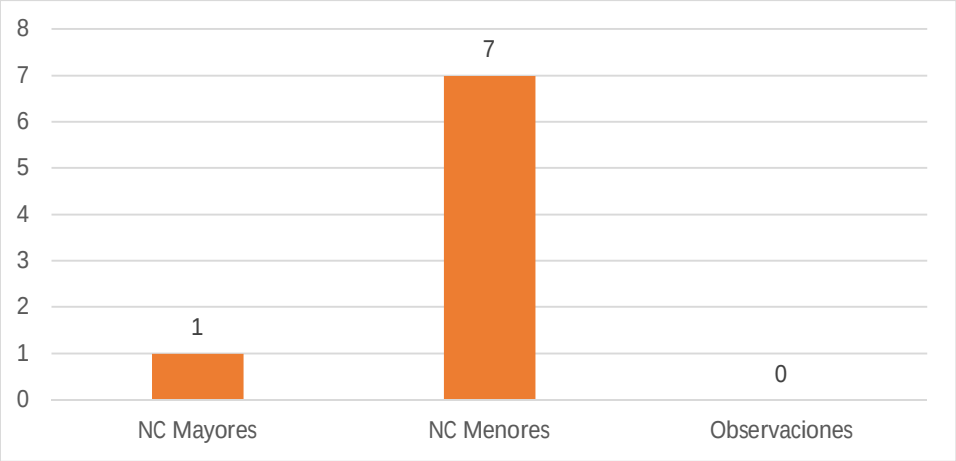


Ilustración 47. No Cumplimientos Cunplimiento Legal

20. Anexo XIII. No Conformidades con la Norma ISO 27002:2013

Dominio		Aspectos organizativos de la seguridad de la información			
Objetivo de Control		Organización interna			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L1	L2	A.6.1.3 Contacto con las autoridades			
No Conformidad		Aunque se mantienen contactos con las autoridades no se trata de un proceso planificado, supervisado y ajustado).			
Evidencias		No hay evidencias de gestión del rendimiento ni de la gestión de los resultados			
Propuesta de Acciones Correctivas		Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado.			
Auditor		Manuel Jimber[3]	Fecha Aud.	11/12/2015	
Responsable Ejecución		Responsable de Seguridad de la Información	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Comisión de Seguridad de la Información	Firma		

[3] Para todas las "No conformidades" de este anexo aparece como Auditor Manuel Jimber, que durante todo el ejercicio ha actuado como consultor del proyecto. Como es de sobra sabido esta situación no puede darse en un supuesto real, pues se perdería la independencia, resultando que el consultor auditaría su propio trabajo. Al tratarse de un ejercicio lo dejaremos como está teniendo en cuenta esta circunstancia.

Dominio		Seguridad ligada a los recursos humanos			
Objetivo de Control		Cese o cambio de puesto de trabajo			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L0	L2	A.7.3.1 Cese o cambio de puesto de trabajo			
No Conformidad		No se han establecido las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste.			
Evidencias		No hay			
Propuesta de Acciones Correctivas		Se deberían establecer las responsabilidades para asegurar que el abandono de la organización por parte de los empleados, contratistas o terceras personas se controla, que se devuelve todo el equipamiento y se eliminan completamente todos los derechos de acceso. Los cambios en las responsabilidades y empleos en la organización deberían gestionarse La devolución de los activos de la organización cuando un empleado se marcha sería mucho más sencilla de verificar si el inventario de activos ha sido actualizado y verificado regularmente. Determinar los accesos que necesitan revocarse en primer lugar cuando un empleado presenta su carta de dimisión: ¿cuáles son los sistemas más críticos o vulnerables? Hacer un seguimiento del uso del e-mail por estas personas antes de salir definitivamente de la empresa, por si comienzan a sacar información confidencial (sujeto a las políticas aplicables y a consideraciones legales sobre privacidad).			
Auditor		Manuel Jimber	Fecha Aud.	11/12/2015	
Responsable Ejecución		Dirección de Recursos Humanos Dirección TIC	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Comisión de Seguridad de la Información	Firma		

Dominio		Gestión de activos			
Objetivo de Control		Responsabilidad sobre los activos			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L1	L2	A.8.1.1 Inventario de activos A.8.1.2 Propiedad de los activos A.8.1.4 Devolución de activos			
No Conformidad		Aunque hay procedimiento de gestión de activos, inventario y se han definido los propietarios no se trata de un proceso gestionado			
Evidencias		No se ha evidenciado la definición de objetivos del proceso ni las responsabilidades de su ejecución. El rendimiento del proceso no está supervisado.			
Propuesta de Acciones Correctivas		Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado.			
Auditor		Manuel Jimber	Fecha Aud.	11/12/2015	
Responsable Ejecución		Dirección TIC	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Dirección Gerencia	Firma		

Dominio		Gestión de activos			
Objetivo de Control		Clasificación de la información			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L1	L2	A.8.2.1 Directrices de clasificación A.8.2.2 Etiquetado y manipulado de la información A.8.2.3 Manipulación de activos			
No Conformidad		Aunque hay procedimiento de clasificación y etiquetado de la información, no se trata de un proceso gestionado			
Evidencias		No se ha evidenciado la definición de objetivos del proceso ni las responsabilidades de su ejecución. El rendimiento del proceso no está supervisado.			
Propuesta de Acciones Correctivas		Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado.			
Auditor		Manuel Jimber	Fecha Aud.	11/12/2015	
Responsable Ejecución		Servicio de Atención en Urgencias Responsable de Seguridad de la Información	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Comisión de Seguridad de la Información	Firma		

Dominio		Gestión de activos			
Objetivo de Control		Manejo de los soportes de almacenamiento			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L0	L2	A.8.3.1 Gestión de soportes extraíbles A.8.3.2 Eliminación de soportes A.8.3.3 Soportes físicos en tránsito			
No Conformidad		Aunque hay procedimiento de gestión de soportes, no se trata de un proceso gestionado.			
Evidencias		No se ha evidenciado la definición de objetivos del proceso ni las responsabilidades de su ejecución. El rendimiento del proceso no está supervisado. No hay procedimiento de Soportes físicos en tránsito			
Propuesta de Acciones Correctivas		Se deberían proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los limites físicos de la organización. Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado.			
Auditor		Manuel Jimber	Fecha Aud.	11/12/2015	
Responsable Ejecución		Dirección TIC Servicio de Atención en Urgencias	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Comisión de Seguridad de la Información	Firma		

Dominio		Control de accesos			
Objetivo de Control		Requisitos de negocio para el control de accesos			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L1	L2	A.9.1.1 Política de control de accesos. A.9.1.2 Control de acceso a las redes y servicios asociados.			
No Conformidad		Aunque se han definido los requisitos del negocio para el control de acceso no se han encontrado evidencias de gestión del rendimiento ni gestión de los resultados del proceso.			
Evidencias		El procedimiento de control de accesos no incluye objetivos de rendimiento ni el proceso de supervisión del mismo.			
Propuesta de Acciones Correctivas		Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado.			
Auditor		Manuel Jimber	Fecha Aud.	11/12/2015	
Responsable Ejecución		Servicio de Atenicón en Urgencias Dirección TIC	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Comisión de Seguridad de la Información	Firma		

Dominio		Control de accesos			
Objetivo de Control		Gestión de acceso de usuario			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L0	L2	A.9.2.1 Gestión de altas/bajas en el registro de usuarios A.9.2.2 Gestión de los derechos de acceso asignados a usuarios A.9.2.3 Gestión de los derechos de acceso con privilegios especiales A.9.2.4 Gestión de información confidencial de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de los usuarios A.9.2.6 Retirada o adaptación de los derechos de acceso			
No Conformidad		Aunque el proceso de gestión de acceso de usuario contempla altas y bajas y la gestión de los derechos asignados a los usuarios tiene deficiencias y no cumple con su objetivo			
Evidencias		El proceso de gestión de accesos a usuario no contempla la gestión de derechos de usuarios especiales, gestión confidencial de autenticación de usuarios, revisión de los derechos de acceso y retirada o adaptación de los derechos de acceso.			
Propuesta de Acciones Correctivas		La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado. La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado. Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios. Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio. Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado.			
Auditor		Manuel Jimber	Fecha Aud.	11/12/2015	
Responsable Ejecución		Dirección TIC Dirección de Recursos Humanos	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Comisión de Seguridad de la Información	Firma		

Dominio		Control de accesos			
Objetivo de Control		Responsabilidades del usuario.			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L1	L2	A.9.3.1 Uso de información confidencial para la autenticación.			
No Conformidad		Aunque se han definido las prácticas de seguridad para el uso confidencial de la información para la autenticación no se trata de un proceso gestionado.			
Evidencias		No se ha evidenciado la definición de objetivos de rendimiento ni el proceso de supervisión del mismo.			
Propuesta de Acciones Correctivas		Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado.			
Auditor		Manuel Jimber	Fecha Aud.	11/12/2015	
Responsable Ejecución		Dirección TIC	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Comisión de Seguridad de la Información	Firma		

Dominio		Control de accesos			
Objetivo de Control		Control de acceso a sistemas y aplicaciones.			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L1	L2	A.9.4.1 Restricción del acceso a la información. A.9.4.2 Procedimientos seguros de inicio de sesión. A.9.4.3 Gestión de contraseñas de usuario. A.9.4.4 Uso de herramientas de administración de sistemas. A.9.4.5 Control de acceso al código fuente de los programas.			
No Conformidad		Aunque se han definido los procesos de control de acceso a sistemas y aplicaciones no se trata de un proceso gestionado.			
Evidencias		No se ha evidenciado la definición de objetivos de rendimiento ni el proceso de supervisión del mismo.			
Propuesta de Acciones Correctivas		Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado.			
Auditor		Manuel Jimber	Fecha Aud.	11/12/2015	
Responsable Ejecución		Dirección TIC	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Comisión de Seguridad de la Información	Firma		

Dominio		Cifrado			
Objetivo de Control		Controles criptográficos			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L1	L2	A.10.1.1 Política de uso de los controles criptográficos. A.10.1.2 Gestión de claves.			
No Conformidad		Aunque se han definido los procesos de controles criptográficos. no se trata de un proceso gestionado.			
Evidencias		No se ha evidenciado la definición de objetivos de rendimiento ni el proceso de supervisión del mismo.			
Propuesta de Acciones Correctivas		Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado.			
Auditor		Manuel Jimber	Fecha Aud.	11/12/2015	
Responsable Ejecución		Dirección TIC	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Comisión de Seguridad de la Información	Firma		

Dominio		Seguridad física y ambiental			
Objetivo de Control		Áreas seguras			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L1	L2	A.11.1.1 Perímetro de seguridad física. A.11.1.2 Controles físicos de entrada. A.11.1.3 Seguridad de oficinas, despachos y recursos. A.11.1.5 El trabajo en áreas seguras.			
No Conformidad		Aunque se han definido los procesos de las Áreas seguras, no se trata de un proceso gestionado			
Evidencias		Hay evidencias de proceso gestionado para la protección contra las amenazas externas y ambientales y las áreas de acceso público, carga y descarga. Sin embargo no sucede lo mismo con los procesos relacionados con el perímetro de seguridad física, Controles físicos de entrada, Seguridad de oficinas, despachos y recursos, El trabajo en áreas seguras.			
Propuesta de Acciones Correctivas		Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado.			
Auditor		Manuel Jimber	Fecha Aud.	11/12/2015	
Responsable Ejecución		Dirección TIC	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Comisión de Seguridad de la Información	Firma		

<table>
<tr><td colspan="2">Dominio</td><td colspan="4">Seguridad física y ambiental</td></tr>
<tr><td colspan="2">Objetivo de Control</td><td colspan="4">Seguridad de los equipos.</td></tr>
<tr><td>Nivel de Madurez</td><td>Nivel Objetivo</td><td>Controles</td><td>Tipo No Conformidad</td><td>MAYOR</td><td></td></tr>
<tr><td rowspan="2">L1</td><td rowspan="2">L2</td><td rowspan="2">A.11.2.3 Seguridad del cableado.
A.11.2.5 Salida de activos fuera de las dependencias de la empresa.
A.11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.</td><td></td><td>MENOR</td><td></td></tr>
<tr><td colspan="2">No Conformidad</td><td colspan="4">Aunque se han definido los procesos para la seguridad de los equipos, no se trata de un proceso gestionado</td></tr>
<tr><td colspan="2">Evidencias</td><td colspan="4">No hay evidencias de proceso gestionado para la seguridad del cableado.
No hay procedimientos definidos para la salida de activos fuera de las dependencias de la empresa y la seguridad de los equipos y activos fuera de las instalaciones.</td></tr>
<tr><td colspan="2">Propuesta de Acciones Correctivas</td><td colspan="4">Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado.
Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger contra la intercepción, interferencia o posibles daños.
Los equipos, la información o el software no se deberían retirar del sitio sin previa autorización.
Se debería aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos.</td></tr>
<tr><td colspan="2">Auditor</td><td colspan="2">Manuel Jimber</td><td>Fecha Aud.</td><td>11/12/2015</td></tr>
<tr><td colspan="2" rowspan="2">Responsable Ejecución</td><td colspan="2" rowspan="2">Dirección TIC</td><td>Fecha Rev.</td><td>11/12/2016</td></tr>
<tr><td colspan="2">Firma</td></tr>
<tr><td colspan="2" rowspan="2">Responsable Aceptación</td><td colspan="2" rowspan="2">Comisión de Seguridad de la Información</td><td colspan="2">Firma</td></tr>
<tr><td colspan="2"></td></tr>
</table>

Dominio		Seguridad en la operativa			
Objetivo de Control		Responsabilidades y procedimientos de operación			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L0	L2	A.12.1.1 Documentación de procedimientos de operación. A.12.1.2 Gestión de cambios. A.12.1.3 Gestión de capacidades. A.12.1.4 Separación de entornos de desarrollo, prueba y producción.			
No Conformidad		Aunque se han definido los procesos para la seguridad de los equipos, no se trata de un proceso gestionado. No se ha definido un procedimiento de Gestión de cambios.			
Evidencias		No se ha definido un procedimiento de Gestión de cambios			
Propuesta de Acciones Correctivas		Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado. Se deberían controlar los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información.			
Auditor		Manuel Jimber	Fecha Aud.	11/12/2015	
Responsable Ejecución		Dirección TIC	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Comisión de Seguridad de la Información	Firma		

Dominio		Seguridad en la operativa			
Objetivo de Control		Registro de actividad y supervisión			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L2	L2	A.12.4.4 Sincronización de relojes.			
No Conformidad		El procedimiento de sincronización de relojes no es un proceso gestionado			
Evidencias		No se ha evidenciado la definición de objetivos de rendimiento del proceso ni la supervisión del mismo			
Propuesta de Acciones Correctivas		Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado.			
Auditor		Manuel Jimber	Fecha Aud.	11/12/2015	
Responsable Ejecución		Dirección TIC	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Comisión de Seguridad de la Información	Firma		

Dominio		Seguridad en la operativa			
Objetivo de Control		Control del software en explotación			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L1	L2	A.12.5.1 Instalación del software en sistemas en producción.			
No Conformidad		El procedimiento de instalación del software en sistemas en producción no es un proceso gestionado			
Evidencias		No se ha evidenciado la definición de objetivos de rendimiento del proceso ni la supervisión del mismo.			
Propuesta de Acciones Correctivas		Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado.			
Auditor		Manuel Jimber	Fecha Aud.	11/12/2015	
Responsable Ejecución		Dirección TIC	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Comisión de Seguridad de la Información	Firma		

Dominio		Seguridad en la operativa			
Objetivo de Control		Gestión de la vulnerabilidad técnica.			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L1	L2	A.12.6.1 Gestión de las vulnerabilidades técnicas. A.12.6.2 Restricciones en la instalación de software.			
No Conformidad		El procedimiento de Gestión de la vulnerabilidad técnica no es un proceso gestionado			
Evidencias		No se ha evidenciado la definición de objetivos de rendimiento del proceso ni la supervisión del mismo.			
Propuesta de Acciones Correctivas		Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado.			
Auditor		Manuel Jimber	Fecha Aud.	11/12/2015	
Responsable Ejecución		Dirección TIC	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Comisión de Seguridad de la Información	Firma		

Dominio		Seguridad en las telecomunicaciones			
Objetivo de Control		Gestión de la seguridad en las redes			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L1	L2	A.13.1.3 Segregación de redes.			
No Conformidad		El procedimiento de Segregación de redes no es un proceso gestionado			
Evidencias		No se ha evidenciado la definición de objetivos de rendimiento del proceso ni la supervisión del mismo.			
Propuesta de Acciones Correctivas		Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado.			
Auditor		Manuel Jimber	Fecha Aud.	11/12/2015	
Responsable Ejecución		Dirección TIC	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Comisión de Seguridad de la Información	Firma		

Dominio		Seguridad en las telecomunicaciones			
Objetivo de Control		Intercambio de información con partes externas.			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L1	L2	A.13.2.1 Políticas y procedimientos de intercambio de información. A.13.2.2 Acuerdos de intercambio. A.13.2.3 Mensajería electrónica. A.13.2.4 Acuerdos de confidencialidad y secreto.			
No Conformidad		El procedimiento Intercambio de información con partes externas no es un proceso gestionado			
Evidencias		No se ha evidenciado la definición de objetivos de rendimiento del proceso ni la supervisión del mismo			
Propuesta de Acciones Correctivas		Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado.			
Auditor		Manuel Jimber	Fecha Aud.	11/12/2015	
Responsable Ejecución		Dirección TIC	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Comisión de Seguridad de la Información	Firma		

Dominio		Adquisición, desarrollo y mantenimiento de los sistemas de información			
Objetivo de Control		Requisitos de seguridad de los sistemas de información			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L1	L2	A.14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.			
No Conformidad		El procedimiento de Seguridad de las comunicaciones en servicios accesibles por redes públicas no es un proceso gestionado			
Evidencias		No se ha evidenciado la definición de objetivos de rendimiento del proceso ni la supervisión del mismo			
Propuesta de Acciones Correctivas		Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado.			
Auditor		Manuel Jimber	Fecha Aud.	11/12/2015	
Responsable Ejecución		Dirección TIC	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Comisión de Seguridad de la Información	Firma		

Dominio		Adquisición, desarrollo y mantenimiento de los sistemas de información			
Objetivo de Control		Seguridad en los procesos de desarrollo y soporte.			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L2	L2	A.14.2.4 Restricciones a los cambios en los paquetes de software. A.14.2.5 Uso de principios de ingeniería en protección de sistemas.			
No Conformidad		Aunque el objetivo de control Requisitos de seguridad de los sistemas de información alcanza una efectividad global del 71% y por tanto el nivel 2, los proceso relacionacionados con Restricciones a los cambios en los paquetes de software y Uso de principios de ingeniería en protección de sistemas se no son procesos gestionados.			
Evidencias		No se ha evidenciado la definición de objetivos de rendimiento de los procesos mencionados ni la supervisión de los mismos			
Propuesta de Acciones Correctivas		Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado.			
Auditor		Manuel Jimber	Fecha Aud.	11/12/2015	
Responsable Ejecución		Dirección TIC	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Comisión de Seguridad de la Información	Firma		

<table>
<tr><td colspan="2">Dominio</td><td colspan="4">Relaciones con suministradores</td></tr>
<tr><td colspan="2">Objetivo de Control</td><td colspan="4">Seguridad de la información en las relaciones con suministradores</td></tr>
<tr><td>Nivel de Madurez</td><td>Nivel Objetivo</td><td>Controles</td><td>Tipo No Conformidad</td><td>MAYOR</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td>MENOR</td><td></td></tr>
<tr><td>L0</td><td>L2</td><td colspan="4">A.15.1.1 Política de seguridad de la información para suministradores.
A.15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
A.15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.</td></tr>
<tr><td colspan="2">No Conformidad</td><td colspan="4">El objetivo de control Seguridad de la información en las relaciones con suministradores no alcanza su objetivo</td></tr>
<tr><td colspan="2">Evidencias</td><td colspan="4">No se ha evidenciado la definición de objetivos de rendimiento de las Política de seguridad de la información para suministradores, ni la supervisión de las mismas.
No hay procedimientos definidos para el Tratamiento del riesgo dentro de acuerdos de suministradores y la Cadena de suministro en tecnologías de la información y comunicaciones.</td></tr>
<tr><td colspan="2">Propuesta de Acciones Correctivas</td><td colspan="4">Definir los procedimientos para el Tratamiento del riesgo dentro de acuerdos de suministradores y Tratamiento del riesgo dentro de acuerdos de suministradores.
Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado.</td></tr>
<tr><td colspan="2">Auditor</td><td colspan="2">Manuel Jimber</td><td>Fecha Aud.</td><td>11/12/2015</td></tr>
<tr><td colspan="2" rowspan="2">Responsable Ejecución</td><td colspan="2" rowspan="2">Dirección TIC
Direción Económica</td><td>Fecha Rev.</td><td>11/12/2016</td></tr>
<tr><td colspan="2">Firma</td></tr>
<tr><td colspan="2">Responsable Aceptación</td><td colspan="2">Comisión de Seguridad de la Información</td><td colspan="2">Firma</td></tr>
</table>

Dominio		Relaciones con suministradores			
Objetivo de Control		Gestión de la prestación del servicio por suministradores.			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L0	L2	A.15.2.1 Supervisión y revisión de los servicios prestados por terceros. A.15.2.2 Gestión de cambios en los servicios prestados por terceros.			
No Conformidad		El objetivo de control Gestión de la prestación del servicio por suministradores no alcanza su objetivo			
Evidencias		No se ha evidenciado la existencia de procedimientos para la Supervisión y revisión de los servicios prestados por terceros y la Gestión de cambios en los servicios prestados por terceros.			
Propuesta de Acciones Correctivas		Definir los procesos para la Supervisión y revisión de los servicios prestados por terceros y la Gestión de cambios en los servicios prestados por terceros. Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado			
Auditor		Manuel Jimber	Fecha Aud.	11/12/2015	
Responsable Ejecución		Dirección Económica	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Comisión de Seguridad de la Información	Firma		

Dominio		Cumplimiento			
Objetivo de Control		Gestión de incidentes de seguridad de la información y mejoras.			
Nivel de Madurez	Nivel Objetivo	Controles	Tipo No Conformidad	MAYOR	
				MENOR	
L2	L2	A.18.1.5 Regulación de los controles criptográficos.			
No Conformidad		Aunque el objetivo de control Gestión de incidentes de seguridad de la información y mejoras alcanza globalmente el nivel de madurez de proceso gestionado, el procedimiento de Regulación de los controles criptográficos no está definido			
Evidencias		No se ha evidenciado la definición del procedimiento de Regulación de los controles criptográficos			
Propuesta de Acciones Correctivas		Definir el procedimiento para la Regulación de los controles criptográficos. Definir los objetivos del rendimiento del proceso, las responsabilidades para la ejecución del proceso, y los recursos necesarios. Supervisar el rendimiento del proceso y verificar que se ajusta a lo planificado			
Auditor		Manuel Jimber	Fecha Aud.	11/12/2015	
Responsable Ejecución		Dirección TIC	Fecha Rev.	11/12/2016	
			Firma		
Responsable Aceptación		Comisión de Seguridad de la Información	Firma		