2017

IMPLEMENTACIÓN ISO 27001

TRABAJO FIN DE MÁSTER

CUERVO ALVAREZ, SARA

INDICE

INDICE DE TABLAS&FIGURAS

➢ INTRODUCCION.

El objetivo de este trabajo final de master es la de implantar un plan director de seguridad en una empresa. 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).

Este trabajo se divide en varias partes, como se puede observar en el índice:

- En primer lugar, tenemos, la introducción al proyecto sobre el que se va a trabajar, enfoque y selección de la empresa con la que se va a trabajar y por último la definición de los objetivos del plan de seguridad y el análisis diferencial de la empresa, y siempre de acuerdo con las normas ISO27001 y ISO 27002.
- En segundo lugar, tenemos, el sistema de gestión documental. En este punto se definirán la política de seguridad, la declaración de aplicabilidad y la documentación necesaria para el SGSI.
- En tercer lugar, se deberá llevar a cabo la elaboración de la metodología de análisis de riesgos.
- En cuarto lugar, tendrá lugar la propuesta de proyectos. En este punto se evaluarán proyectos que se deben llevar a cabo en la organización para alinearlo con los objetivos planteados en el plan director de seguridad, así como la cuantificación económica y temporal de los mismos.
- En quinto lugar, tendrá lugar la evaluación de controles, madurez de los mismos, así como el nivel de cumplimiento.
- En sexto y último lugar, se consolidarán los resultados obtenidos durante el proceso de análisis, así como la realización de los informes y presentación ejecutiva a la dirección.

➢ SITUACION ACTUAL: CONTEXTUALIZACION, OBJETIVOS Y ANALISIS DIFERENCIAL

a. Contextualización.

En 1959, dos analistas de computadoras juntaron $ 100 para formar FICTICIA, S.A, proporcionando a los fabricantes de computadoras complejos programas conocidos como ensambladores, compiladores y sistemas operativos. Durante las cinco décadas siguientes, FICTICIA, S.A creció rápidamente para servir a gobiernos y empresas de todo el mundo.

En 1962 se fundó la compañía, pioneros en outsourcing de TI, la compañía inicial creció desde la inversión inicial de $ 1.000 a una empresa global que ayudó a 500 millones de pasajeros a bordo de aviones, procesó 13 mil millones de transacciones de tarjetas de crédito y realizó 2.400 millones de transacciones de atención médica.

Esta compañía llega a nuestra comunidad alrededor de los años noventa, de la mano de una de las mayores multinacionales extranjeras de la época. Actúa como proveedor tecnológico de soluciones empresariales y servicio, dando a los clientes soluciones que se adapten en todo momento a sus necesidades. Una de las principales características de este centro es la de poder dar soporte hasta en 9 idiomas diferentes puesto que sus principales clientes son multinacionales como aseguradoras, fabricantes de automóviles, firmas de telecomunicaciones, además de instituciones públicas.

Es una compañía que ya ha tenido sus primeros contactos con la ISO 27001 puesto que ya ha certificado una de sus oficinas. Pero actualmente está en un importante punto de mejora de todas sus políticas, procedimientos, etc … Su objetivo principal es la de expandirse a una nueva oficina y certificarla bajo la normal ISO27001.

Los principales servicios que esta compañía proporciona son: servicios de aplicaciones, servicios en la nube, consultoría, seguridad, banca, seguros, sector público global.

Algunos de los departamentos en los que se divide son:

- Tecnologías web.
- Testeos
- Tecnologías emergentes.
- SAP-Oracle
- Middleware
- Mainframe

- Bases de datos
- Big Data.

1) Alcance:

Los sistemas de información que dan soporte a los diferentes puntos que se indican a continuación según la declaración de aplicabilidad vigente:

- ✓ Todos los recursos humanos que se vean implicados directa o indirectamente con el negocio de Asturias.
- ✓ Todos los servidores (producción, testeo, desarrollo), aplicaciones que se manejen o controlen desde nuestro emplazamiento.
- ✓ Todos los activos de información durante toda su vida útil hasta su eliminación (en formato electrónico o físico para el caso de ordenadores, móviles, etc …).
- ✓ Toda la información generada durante la vida del negocio para los proyectos.
- ✓ La información de empleados, clientes, proveedores de servicios, etc

b. Conociendo la ISO 27001 – ISO 27002

- **ISO 27001**

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

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001. ISO 27001 se ha convertido en la

principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento.

- **¿Cómo funciona?**

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software, pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI).

Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, anti-virus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc.

➢ ¿Por qué ISO 27001 es importante para la empresa?

Hay 4 ventajas comerciales esenciales que una empresa puede obtener con la implementación de esta norma para la seguridad de la información:

- Cumplir con los requerimientos legales – cada vez hay más y más leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información. La buena noticia es que la mayoría de ellos se pueden resolver implementando ISO 27001 ya que esta norma le proporciona una metodología perfecta para cumplir con todos ellos.
- Obtener una ventaja comercial – si su empresa obtiene la certificación y sus competidores no, es posible que usted obtenga una ventaja sobre ellos ante los ojos de los clientes a los que les interesa mantener en forma segura su información.
- Menores costos – la filosofía principal de ISO 27001 es evitar que se produzcan incidentes de seguridad, y cada incidente, ya sea grande o pequeño, cuesta dinero; por lo tanto, evitándolos su empresa va a ahorrar mucho dinero. Y lo mejor de todo es que la inversión en ISO 27001 es mucho menor que el ahorro que obtendrá.
- Una mejor organización – en general, las empresas de rápido crecimiento no tienen tiempo para hacer una pausa y definir sus procesos y procedimientos; como consecuencia, muchas veces los empleados no saben qué hay que hacer, cuándo y quién debe hacerlo. La implementación de ISO 27001 ayuda a resolver este tipo de situaciones ya que alienta a las empresas a escribir sus principales procesos (incluso los que no están relacionados con la seguridad), lo que les permite reducir el tiempo perdido de sus empleados.

➢ ¿Cómo implementar ISO 27001?

Para implementar la norma ISO 27001 en una empresa, usted tiene que seguir estos 16 pasos:

1) Obtener el apoyo de la dirección
2) Utilizar una metodología para gestión de proyectos
3) Definir el alcance del SGSI
4) Redactar una política de alto nivel sobre seguridad de la información
5) Definir la metodología de evaluación de riesgos
6) Realizar la evaluación y el tratamiento de riesgos
7) Redactar la Declaración de aplicabilidad

8) Redactar el Plan de tratamiento de riesgos

9) Definir la forma de medir la efectividad de sus controles y de su SGSI

10) Implementar todos los controles y procedimientos necesarios

11) Implementar programas de capacitación y concienciación

12) Realizar todas las operaciones diarias establecidas en la documentación de su SGSI

13) Monitorear y medir su SGSI

14) Realizar la auditoría interna

15) Realizar la revisión por parte de la dirección

16) Implementar medidas correctivas

➢ Fases del sistema de gestión

La norma ISO 27001 determina cómo gestionar la seguridad de la información a través de un sistema de gestión de seguridad de la información está formado por cuatro fases que se deben implementar en forma constante para reducir al mínimo los riesgos sobre confidencialidad, integridad y disponibilidad de la información. Las fases son las siguientes:

- La Fase de planificación: esta fase sirve para planificar la organización básica y establecer los objetivos de la seguridad de la información y para escoger los controles adecuados de seguridad (la norma contiene un catálogo de 133 posibles controles).
- La Fase de implementación: esta fase implica la realización de todo lo planificado en la fase anterior.
- La Fase de revisión: el objetivo de esta fase es monitorear el funcionamiento del SGSI mediante diversos “canales” y verificar si los resultados cumplen los objetivos establecidos.
- La Fase de mantenimiento y mejora: el objetivo de esta fase es mejorar todos los incumplimientos detectados en la fase anterior.
- El ciclo de estas cuatro fases nunca termina, todas las actividades deben ser implementadas cíclicamente para mantener la eficacia del SGSI.

▪ ISO 27002

La norma ISO 27002 fue publicada originalmente como un cambio de nombre de la norma ISO 17799, la cual se basaba en un documento publicado por el gobierno del Reino Unido, que se convirtió en estándar en 1995. Fue en el 2000 cuando se publicó por primera vez como ISO 17799, y en 2005 aparece una nueva versión, junto con la publicación de la norma ISO 27001. No debe olvidarse que estos dos documentos están destinados a ser utilizados de forma complementaria.

Dentro de ISO/IEC 27002 se extiende la información de los renovados anexos de ISO/IEC 27001-2013, donde básicamente se describen los dominios de control y los mecanismos de control, que pueden ser implementados dentro de una organización, siguiendo las directrices de ISO 27001. En esta nueva versión de la norma se

encuentran los controles que buscan mitigar el impacto o la posibilidad de ocurrencia de los diferentes riesgos a los cuales se encuentra expuesta la organización.

Con la actualización de esta norma las organizaciones pueden encontrar una guía que sirva para la implementación de los controles de seguridad de la organización y de las prácticas más eficaces para gestionar la seguridad de la información. Aunque antes de pensar en cómo migrar al nuevo estándar ISO/IEC 27001:2013, es importante tener en cuenta que las categorías de los controles se han mezclado un poco, esto buscando que los dominios de control tengan una estructura más coherente.

Dentro de los cambios interesantes de resaltar que lo relacionado con dispositivos móviles y teletrabajo que antes estaba asociado al Control de Accesos, ahora se encuentra dentro de la sección 6 "*Organización de la Seguridad de la Información*". Y dentro de la sección de Control de Accesos se engloba lo relacionado con acceso al sistema operativo, a las aplicaciones y la información. Todo lo relacionado con Criptografía es un dominio de control nuevo, sección 10, dentro de la cual se incluyen todos los controles criptográficos sugeridos para una organización. En el caso de los controles que deben tenerse en cuenta en el caso de la recuperación de desastres están dentro de la sección 17.

Además, cabe resaltar que existen versiones específicas de la norma ISO/IEC 27002, enfocadas en diferentes tipos de empresas: manufactureras, sector de la salud, sector financiero, entre otros. Si bien la nomenclatura ISO es diferente, son normas que toman como referencia la ya mencionada ISO 27002 y por tanto lo tanto están alienados para la correcta gestión de la seguridad de la información.

a. Objetivos del plan director.

Mediante la definición de un plan director de seguridad se pretende conseguir el alineamiento necesario para mantener un buen nivel de seguridad tanto en el edificio principal como en el edificio secundario, consiguiendo de esta manera que para el cliente sea transparente el emplazamiento desde el que se proporciona el servicio.

Los principales objetivos a llevar a cabo serán:

- ✓ Identificar el nivel de seguridad actual del emplazamiento y la inversión necesaria para que cumpla con las expectativas (siempre teniendo en cuentas las exigencias más restrictivas para no tener problema con los clientes más exigentes).
- ✓ Implementación y seguimiento adecuado del plan generado para que se siga correctamente el ciclo de la mejora continua del sistema.
- ✓ Analizar y detallar el 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.

- ✓ Optimizar las soluciones de seguridad que se apliquen en el sistema.
- ✓ Optimizar las inversiones para estas medidas de seguridad.
- ✓ Optimizar el tiempo de recuperación frente a un ataque, ya bien sea en una ubicación alternativa o mediante la desviación de los servicios eficientemente.

b. Análisis diferencial.

Para una estimación inicial se han evaluado algunos de los puntos obligatorios de las normas, así como algunos de los controles de la norma ISO27002. La estimación se ha realizado a alto nivel.

El estado en el que se encuentra cada control se puede analizar en función del porcentaje:

- 0% ➔No aplicado.
- 10% - 50% ➔Fase inicial.
- 50% - 90 % ➔Fase intermedia.
- 100% ➔Completamente integrado.

4	CONTEXTO DE LA ORGANIZACIÓN			%
	4.1		COMPRENSION DE LA ORGANIZACIÓN Y DE SU CONTEXTO	95%
	4.2		COMPRENSION DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	95%
	4.3		DERMINACION DEL ALCANCE DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION	80%
	4.4		SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION	95 %
5				
	5.1		LIDERZGO Y COMPROMISO	90%
	5.2		POLITICA	80 %
	5.3		ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACION	90%
6				
	6.1	ACCIONES PARA TRATAR LOS RIESGOS Y OPORTUNIDADES		
		6.1.1	CONSIDERACIONES GENERALES	95 %
		6.1.2	APRECIACION DE RIESGOS DE SEGURIDADDE LA INFORMACION	95 %
		6.1.3	TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACION	95 %

	6.2		OBJETIVOS DE SEGURIDAD DE LA INFORMACION Y PLANIFICACION PARA SU CONSECUCION	95 %
7				
	7.1		RECURSOS	95 %
	7.2		COMPETENCIA	95 %
	7.3		CONCIENCIACION	95 %
	7.4		COMUNICACION	95 %
	7.5		INFORMACION DOCUMENTADA	95 %
		7.5.1	CONSIDERACIONES GENERALES	95 %
		7.5.2	CREACION Y ACTUALIZACION	95 %
		7.5.3	CONTROL DE LA INFORMACION DOCUMENTADA	95 %
8				
	8.1		PLANIFICACION Y CONTROL OPERACIONAL	95 %
	8.2		APRECIACION DE LOS RIESGOS DE SEGURIDAD DE INFORMACION	95 %
	8.3		TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE INFORMACION	95 %
9				
	9.1		SEGUIMIENTO, MEDICION, ANALISIS Y EVALUACION	95 %
	9.2		AUDITORIA INTERNA	50 %
	9.3		REVISION POR LA DIRECCION	95 %
10	MEJORA			
	10.1		NO CONFORMIDAD Y ACCIONES CORRECTIVAS	50%
	10.2		MEJORA CONTINUA	90%

Tabla 1-A: Análisis puntos iso 27001

5	POLITICAS DE SEGURIDAD			%	COMENTARIO
	5.1	DIRECTRICES DE LA DIRECCION EN SEGURIDAD DE L A INFORMACION			
		5.1.1	CONJUNTO DE POLITICAS PARA LA SEGURIDAD DE LA INFORMACION	80%	
		5.1.2	REVISION DE LAS POLITICAS PARA LA SEGURIDAD DE LA INFORMACION	80%	
6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION				

	6.1	ORGANIZACIÓN INTERNA			
		6.1.1	ASIGNACION DE RESPONSABILIDADES PARA LA SEG DE LA INFORMACION	95%	
		6.1.2	SEGREGACION DE TAREAS	95 %	
		6.1.3	CONTACTO CON LAS AUTORIDADES	95%	
		6.1.4	CONTACTO CON GRUPOS DE INTERES ESPECIAL	95%	
		6.1.5	SEGURIDAD DE LA INFORMACION EN LA GESTION DE PROYECTOS	95%	
	6.2	DISPOSITIVOS PARA MOVILIDAD Y TELETRABAJO			
		6.2.1	POLITICA DE USO DE DISPOSITIVOS PARA MOVILIDAD	80%	
		6.2.2	TELETRABAJO	80%	
7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS				
	7.1	ANTES DE LA CONTRATACION			
		7.1.1	INVESTIGACION DE ANTECEDENTES	80%	
		7.1.2	TERMINOS Y CONDICIONES DE CONTRATACION	95%	
	7.2	DURANTE LA CONTRATACION			
		7.2.1	RESPONSABILIDADES DE GESTION	95%	
		7.2.2	CONCIENCIACION, EDUCACION Y CAPACIDATACION EN SEG. DE LA INF.	95%	
		7.2.3	PROCESO DISCIPLINARIO	95%	
	7.3	CESE O CAMBIO DE PUESTO DE TRABAJO			
		7.3.1	CESE O CAMBIO DE PUESTO DE TRABAJO	95%	
8	GESTION DE ACTIVOS				
	8.1	RESPONSABILIDAD SOBRE LOS ACTIVOS			
		8.1.1	INVENTARIO DE ACTIVOS	80%	Coordinar adecuadamente la gestión de activos en el nuevo emplazamiento.
		8.1.2	PROPIEDAD DE LOS ACTIVOS	80%	
		8.1.3	USO ACEPTABLE DE LOS ACTIVOS	80%	
		8.1.4	DEVOLUCION DE LOS ACTIVOS	80%	
	8.2	CLASIFICACION DE LA INFORMACION			
		8.2.1	DIRECTRICES DE CLASIFICACION	95%	
		8.2.2	ETIQUETADO Y MANIPILADO DE LA INFORMACION	95%	
		8.2.3	MANIPULACION DE ACTIVOS	95%	
	8.3	MANEJO DE LOS SOPORTES DE ALMACENAMIENTO			

		8.3.1	GESTION DE SOPORTES EXTRAIBLES	50%	
		8.3.2	ELIMINACION DE SOPORTES	50%	
		8.3.3	SOPORTES FISICOS EN TRANSITO	50%	
9	CONTROL DE ACCESOS				
	9.1	REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS			
		9.1.1	POLITICA DE CONTROL DE ACCESOS	95%	
		9.1.2	CONTORL DE ACCEO A LAS REDES Y SERVICIOS ASOCIADOS	95%	
	9.2	GESTION DE ACCESO DE USUARIO			
		9.2.1	GESTION DE ALTAS/BAJAS EN EL REGISTRO DE USUARIOS	95%	
		9.2.2	GESTION DE LOS DERECJOS DE ACCEOS ASIGNADOS A USUARIOS	95%	
		9.2.3	GESTION DE LOS DERECHOS DE ACCESO CON PRIVILEGIOS ESPECIALES	95%	
		9.2.4	GESTION DE INFORMACION CONFIDENCIAL DE AUTENTICACION DE USUSARIOS	95%	
		9.2.5	REVISION DE LOS DERECHOS DE ACCESO DE LOS USUARIOS	95%	
		9.2.6	RETIRADO O ADAPTACION DE LOS DERECHOS DE ACCESO	95%	
	9.3	RESPONSABILIDADES DEL USUARIO			
		9.3.1	USO DE INFORMACION CONFIDENCIAL PARA LA AUTENTICACION	95%	
	9.4	CONTROL DE ACCESO A SISTEMAS Y APLICACIONES			
		9.4.1	RESTRICCION DEL ACCESO A LA INFORMACION	95%	
		9.4.2	PROCEDIMIENTOS SEGUROS DE INICIO DE SESION	95%	
		9.4.3	CUESTION DE CONTRASEÑAS DE USUARIO	95%	
		9.4.4	USO DE HERRAMIENTAS DE ADMINISTRACION DE SISTEMAS	95%	
		9.4.5	CONTROL DE ACCESO AL CODIGO FUENTE DE LOS PROGRAMAS	95%	
10	CIFRADO				
	10.1	CONTROLES CRIPTOGRAFICOS			
		10.1.1	POLITICA DE USO DE LOS CONTROLES CRIPTOGRAFICOS	95%	
		10.1.2	GESTION DE CLAVES	95%	
11	SEGURIDAD FISICA Y AMBIENTAL				
	11.1	AREAS SEGURIDAS			

		11.1.1	PERIMETRO DE SEGURIDAD FISICA	20%	
		11.1.2	CONTROLES FISICOS DE ENTRADA	20%	
		11.1.3	SEGURIDAD DE OFICINAS, DESPACHOS Y RECURSOS	20%	
		11.1.4	PROTECCION CONTRA LAS AMENAZAS EXTERNAS Y AMBIENTALES	20%	
		11.1.5	EL TRABAJO EN AREAS SEGURAS	95%	
		11.1.6	AREAS DE ACCESO PUBLICO, CARGA Y DESCARGA	95%	
	11.2	SEGURIDAD DE LOS EQUIPOS			
		11.2.1	EMPLAZAMIENTO Y PROTECCION DE EQUIPOS	95%	
		11.2.2	INSTALACIONES DE SUMINISTRO	95%	
		11.2.3	SEGURIDAD DEL CABLEADO	95%	
		11.2.4	MANTENIMIENTO DE LOS EQUIPOS	95%	
		11.2.5	SALIDA DE ACTIVOS FUERA DE LAS DEPENDENCIAS DE LA EMPRESA	95%	
		11.2.6	SEGURIDAD DE LOS EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES	95%	
		11.2.7	REUTILIZACION O RETIRADA SEGURDA DE DISPOSITIVOS DE ALMACENAMIENTO	95%	
		11.2.8	EQUIPO INFORMATICO DE USUARIO DESATENDIDO	95%	
		11.2.9	POLITICA DE PUESTO DE TRABAJO DESPEJADO Y BLOQUEO DE PANTALLA	95%	
12	SEGURIDAD EN LA OPERATIVA				
	12.1	RESPONSABILIDADES Y PROCEDIMIENTO DE OPERACIÓN			
		12.1.1	DOCUMENTACION DE PROCEDIMIENTO DE OPERACION	95%	
		12.1.2	GESTION DE CAMBIOS	95%	
		12.1.3	GESTION DE CAPACIDADES	95%	
		12.1.4	SEPARACION DE ENTORNOS DE DESARROLLO, PRUEBA Y PRODUCCION	95%	
	12.2	PROTECCION CONTRA CODIGO MALICIOSO			
		12.2.1	CONTROLES CONTRA EL CODIGO MALICIOSO	95%	
	12.3	COPIAS DE SEGURIDAD			
		12.3.1	COPIAS DE SEGURIDAD DE LA INFORMACION	50%	
	12.4	REGISTRO DE ACTIVIDAD Y SUPERVISION			
		12.4.1	REGISTRO Y GESTION DE EVENTOS DE ACTIVIDAD	95%	
		12.4.2	PROTECCION DE LOS REGISTROS DE INFORMACION	95%	

		12.4.3	REGISTROS DE ACTIVIDAD DEL ADMINISTRADOR Y OPERADOR DEL SISTEMA	95%	
		12.4.4	SINCRONIZACION DE RELOJES	95%	
	12.5	CONTROL DE SOFTWARE EN EXPLOTACION			
		12.5.1	INSTALACION DEL SOFTWARE EN SISTEMAS EN PRODUCCION	95%	
	12.6	GESTION DE LA VULNERABILIDAD TECNICA			
		12.6.1	GESTION DE LAS VULNERABILIDADES TECNICAS	95%	
		12.6.2	RESTRICCIONES EN LA INSTALACION DE SOFTWARE	95%	
	12.7	CONSIDERACIONES DE LAS AUDITORIAS DE LOS SISTEMAS DE INFORMACION			
		12.7.1	CONTROLES DE AUDITORIA DE LOS SISTEMAS DE INFORMACION	95%	
13	SEGURIDAD EN LAS TELECOMUNICACIONES				
	13.1	GESTION DE LA SEGURIDAD EN LAS REDES			
		13.1.1	CONTROLES DE RED	95%	
		13.1.2	MECANISMOS DE SEGURIDAD ASOCIADOS A SERVICIOS EN RED	95%	
		13.1.3	SEGREGACION DE REDES	95%	
	13.2	INTERCAMBIO DE INFORMACION CON PARTES EXTERNAS			
		13.2.1	POLITICAS Y PROCEDIMIENTOS DE INTERCAMBIO DE INFORMACION	95%	
		13.2.2	ACERDOS DE INTERCAMBIO	95%	
		13.2.3	MENSAJERIA ELECTRONICA	95%	
		13.2.4	ACUERDOS DE CONFIDENCIALIDAD Y SECRETO	95%	
14	ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION				
	14.1	REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACION			
		14.1.1	ANALISIS Y ESPECIFICACION DE LOS REQUISITOS DE SEGURIDAD	95%	
		14.1.2	SEGURIDAD DE LAS COMUNICACIONES EN SERVICIOS ACCESIBLES POR REDES PUBLICAS	95%	
		14.1.3	PROTECCION DE LAS TRANSACCIONES POR REDES TELEMATICAS	95%	
	14.2	SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE			
		14.2.1	POLITICA DE DESARROLLO DE SOFTWARE	95%	
		14.2.2	PROCEDIMIENTOS DE CONTROL DE CAMBIOS EN LOS SISTEMAS	95%	
		14.2.3	REVISION TECNICA DE LAS APLICACIONES TRAS EFECTUAR CAMBIOS EN EL SISTEMA OPERATIVO	80%	

		14.2.4	RESTRICCIONES A LOS CAMBIOS EN LOS PAQUETES DE SOFTWARE	80%	
		14.2.5	USO DE PRINCIPIOS DE INGENIERIA EN PROTECCION DE SISTEMAS	95%	
		14.2.6	SEGURIDAD EN ENTORNOS DE DESARROLLO	95%	
		14.2.7	EXTERNALIZACION DEL DESARROLLO DE SOFTWARE	95%	
		14.2.8	PRUEBAS DE FUNCIONALIDAD DURANTE EL DESARROLLO DE LOS SISTEMAS	95%	
		14.2.9	PRUEBAS DE ACEPTACION	95%	
	14.3	DATOS DE PRUEBA			
		14.3.1	PROTECCION DE LOS DATOS UTILIZADOS EN PRUEBAS	95%	
15	RELACIONES CON SUMINISTRADORES				
	15.1	SEGURIDAD DE LA INFORMACION EN LAS RELACIONES CON SUMINISTRADORES			
		15.1.1	POLITICA DE SEG. DE LA INFORMACION PARA SUMINISTRADORES	50%	
		15.1.2	TRATAMIENTO DEL RIESGO DENTRO DE ACUERDOS DE SUMINISTRADORES	50%	
		15.1.3	CADENA DE SUMINISTRO EN TECNOLOGIAS DE LA INF. Y CONMUNICACIONES	50%	
	15.2	GESTION DE LA PRESTACION DEL SERVICIO POR SUMINISTRADORES			
		15.2.1	SUPERVISION Y REVISION DE LOS SERVICIOS PRESTADOS POR TERCEROS	95%	
		15.2.2	GESTION DE CAMBIOS EN LOS SERVICIOS PRESTADOS POR TERCEROS	95%	
16	GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION				
	16.1	GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION Y MEJORAS			
		16.1.1	RESPONSABILIDADES Y PROCEDIMIENTOS	95%	
		16.1.2	NOTIFICACION DE LOS EVENTOS DE SEGURIDAD DE LA INFORMACION	95%	
		16.1.3	NOTIFICACION DE PUNTOS DEBILES DE LA SEGURIDAD	95%	
		16.1.4	VALORACION DE EVENTOS DE SEG. DE LA INF. Y TOMA DE DECISIONES	95%	
		16.1.5	RESPUESTA A LOS INDICES DE SEGURIDAD	95%	
		16.1.6	APRENDIZAJE DE LOS INCIDENTES DE SEG. DE LA INFORMACION	95%	
		16.1.7	RECOPILACION DE EVIDENCIAS	95%	
17	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DEL NEGOCIO				
	17.1	CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION			
		17.1.1	PLANIFICACION DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION	50 %	

		17.1.2	IMPLANTACION DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION	50 %	
		17.1.3	VERIFICACION, REVISION Y EVALUACION DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION.	50 %	
	17.2	REDUNDANCIAS			
		17.2.1	DISPONIBILIDAD DE INSTALACIONES PARA EL PROCESAMIENTO DE LA INFORMACION	50 %	
18	CUMPLIMIENTO				
	18.1	CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES			
		18.1.1	IDENTIFICACION DE LA LEGISLACION APLICABLE	95%	
		18.1.2	DERECHOS DE PROPIEDAD INTELECTUAL(DPI)	95%	
		18.1.3	PROTECCION DE LOS REGISTROS DE LA ORGANIZACIÓN	95%	
		18.1.4	PROTECCION DE DATOS Y PRIVACIDAD DE LA INF. PERSONAL	95%	
		18.1.5	REGULACION DE LOS CONTORLES CRIPTOGRAFICOS	95%	
	18.2	REVISIONES DE LA SEGURIDAD DE LA INFORMACION			
		18.2.1	REVISION INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACION	95%	
		18.2.2	CUMPLIMIENTO DE LAS POLITICAS Y NORMAS DE SEGURIDAD	95%	
		18.2.3	COMPROBACION DEL CUMPLIMIENTO	95%	

Tabla 1-B: Listado de controles ISO 27002

➢ SISTEMA DE GESTION DOCUMENTAL

- **Política de seguridad**.

En este punto se describirá la política de seguridad de la información de la organización.

Por ello el objetivo de la seguridad de la información es garantizar la calidad de la seguridad de la información. Esto se conseguirá por tanto manteniendo las tres características principales de un sistema de gestión de la información, es decir, la confidencialidad, integridad y disponibilidad del sistema.

Esto implica que tanto la organización como toda la plantilla deban actuar siempre o en la medida de lo posible acorde a la política de seguridad de la información, así como también realizar un seguimiento continuo del sistema.

Además, existen otras obligaciones importantes para este estándar a la hora de manejar la política de seguridad de la información. En esta línea la política debe:

- Estar disponible como información documentada.
- Ser comunicada dentro de la organización.
- Estar disponible para las partes interesadas.

Anexo A – Política de Seguridad.

- **Procedimiento de auditorías internas.**

Este documento describe el Procedimiento de Auditoría Interna para el SGSI. El principal objetivo y el alcance de este procedimiento de auditoria interna básicamente se resume en los siguientes puntos:

1.0 PROPOSITO:

1.1 Asegurar que la compañía continúe operando de acuerdo con las políticas, procedimientos y requisitos externos especificados para cumplir con las metas y objetivos de la COMPAÑÍA en relación con su postura de gestión de la seguridad de la información.

1.2 Asegurar que las deficiencias y mejoras al SGSI se identifiquen claramente y cuando sea necesario: de acuerdo con las acciones correctivas requeridas, implementadas y consideradas adecuadas para lograr los objetivos del SGSI y se realiza como parte de un proceso de auditoría interna independiente para asegurar segregación razonable De los derechos.

2.0 ALCANCE:

2.1 Este procedimiento es específico para todas las ubicaciones definidas por el alcance de dicho SGSI e incluye: planificación, ejecución, notificación y requisitos de seguimiento como parte de la auditoría interna del SGSI y se aplica a todos los departamentos y servicios definidos como dentro del alcance del SGSI.

En cuanto al procedimiento general que se debe seguir es el siguiente:

- Se debe mantener un programa de auditoría que refleje todas las auditorías programadas y planeadas para el año calendario de auditoría. Esto incluirá un cronograma de auditorías internas, auditorías realizadas a proveedores, auditoría a realizar por clientes y auditorías de terceros, cuando corresponda.
- Cada lugar sujeto al SGSI de la COMPAÑÍA estará sujeto a una auditoría interna anual. Pueden realizarse auditorías adicionales si un lugar en particular tiene un gran número de conclusiones en su contra.
- Los auditores deben ser independientes de la ubicación en la que están obligados a realizar la auditoría, ya que no tienen obligación de rendir cuentas al centro sujeto a la auditoría.
- Todos los miembros del Equipo de Auditoría Interna serán nombrados por el ISMR.
- El Auditor Principal supervisará la actividad del Equipo de Auditoría.
- Se enviará un plan de auditoría departamento para ser auditado por lo menos tres días hábiles antes de la auditoría.

Para ver con más detalle el procedimiento al completo se deberá comprobar el propio documento.

Anexo B – Procedimiento de auditoria interna.

- **Gestión de indicadores.**

Las métricas o los indicadores es una manera de medir como de eficientes son los controles implementados.

Mediante estas métricas por tanto se busca medir en el caso de esta COMPAÑÍA, métricas sobre los siguientes departamentos/equipos:

- Seguridad física:
    - Mide incidentes en el edificio e infracciones por parte de los empleados.
- Seguridad lógica:
    - Nos dan una visión de cómo de seguro es nuestro sistema.
- Formación en seguridad:
    - Informa del estado de la formación de los nuevos empleados.

		Enero-17	Febrero-17
Seguridad física	Credencial no visible	51	43
	Coches no autorizados a pernoctar	0	0
	Uso no autorizado del parking	0	1
	Coches no registrados	0	0
	Ordenadores desprotegidos	21	23
	Reincidentes	8	8
Formación	Empleados sin formación inicial	0	0
	Empleados sin formación obligatoria	0	0
Seguridad lógica	Malware	0	0
	Aplicaciones P2P	0	0
	Vulnerabilidades(alta)	6	7
	Vulnerabilidades(medio)	23	46
	Vulnerabilidades(baja)	10	9

Tabla 2: Resumen métricas

- **<u>Procedimiento de revisión por la dirección</u>.**

La alta dirección debe revisar el Sistema de Gestión de Seguridad de la Información de la organización a intervalos planificados, para asegurarse de que su conveniencia, adecuación y eficacia son continuas.

La revisión por la dirección debe incluir consideraciones sobre:

- El estado de las acciones con relación a las revisiones previas por la dirección.
- Los cambios en las cuestiones externas e internas que sean pertinentes al Sistema de Gestión de Seguridad de la Información
- Retroalimentación sobre el desempeño de la seguridad de la información
- Retroalimentación de las partes interesadas
- Resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos
- Las oportunidades de mejora continua

Los elementos de salida de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio dentro del Sistema de Gestión de Seguridad de la Información.

La organización debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección.

Esta es la teoría que la ISO 27001 nos proporciona sobre cómo se debe llevar a la práctica las reuniones con la dirección.

En la práctica y en el caso particular de esta empresa ficticia denominada COMPAÑÍA, el seguimiento y /o implicación por parte de la seguridad se realiza:

- Mediante reuniones mensuales de acuerdo a una agenda establecida siguiendo todos los puntos establecidos por la ISO e incorporando en cada ocasión los temas extras que sean necesarios abordar.
- Estas reuniones quedan reflejadas en las notas de reunión de cada mes.
- Estas reuniones también están prefijadas en el calendario oficial de la empresa.

Se adjunta plantilla del acta de reunión →Anexo C.

- **<u>Gestión de roles y responsabilidades</u>.**

La norma también se preocupa porque la alta dirección de una organización asigne responsabilidades y autoridades para cada uno de los roles relativos a la seguridad de la información.

Estas responsabilidades son:

- Asegurarse de que el sistema de gestión de seguridad de la información sea conforme a los requisitos de la norma.
- Informar a la alta dirección sobre el desempeño del sistema de gestión de la seguridad de la información.

Además, como punto de referencia están las diferentes políticas y fuentes de información proporcionadas por la propia empresa a partir del cual y de acuerdo a lo que la norma indica se ha creado el documento de roles y responsabilidades.

Se adjunta de documento de roles y responsabilidades ➔**Anexo D**

- **<u>Declaración de aplicabilidad</u>.**

La declaración de aplicabilidad es uno de los documentos más importantes debido a que es el paso intermedio entre la evaluación y el tratamiento de los riesgos.

El objetivo de este documento es definir qué medidas de seguridad (controles) del anexo de la norma ISO 27001 son lo que se implementaran, y para estos que se implementan como será llevados a cabo.

Como se comentaba al principio este documento es uno de los más importantes debido a que:

- Una vez que se sabe los riesgos a mitigar y los controles que se deben aplicar, pero en este documento se especifican las razones por las que se aplican, es decir, por requisitos de contrato, por razones legales, etc …
- Es una manera viable de resumir y hacer viable de revisar los controles aplicados para los riesgos detectados.
- Al hacer el seguimiento periódico se podrá tener controlado fácilmente que controles están o no aplicados.
    - En el caos de los que estén aplicados se puede ver fácilmente como se ha implementado, es decir, con una política de empresa, con un procedimiento, etc …

<u>Tipo de Requerimientos:</u>

- Legal(L).
- Contractual(C).
- Continuidad de negocio(BC).

▪ Resultado del análisis de riesgos (AR).

5	POLITICAS DE SEGURIDAD	DESCRIPCION	JUSTIFICACION	REQ.	APLICA
5.1	DIRECTRICES DE LA DIRECCION EN SEGURIDAD DE L A INFORMACION				
5.1.1	CONJUNTO DE POLITICAS PARA LA SEGURIDAD DE LA INFORMACION	Se definirá un conjunto de políticas para la seguridad de la información, publicados y comunicados a los empleados ya las partes externas pertinentes.	Función corporativa: El Oficial Principal de Seguridad de la Información aprobará los documentos de política de seguridad de la información, publicará y comunicará a todos los empleados y partes externas relevantes a través del portal.	BC AR	SI
5.1.2	REVISION DE LAS POLITICAS PARA LA SEGURIDAD DE LA INFORMACION	Las políticas de seguridad de la información se revisarán a intervalos planificados o si se producen cambios significativos para asegurar su idoneidad, suficiencia y efectividad.	Función corporativa: se revisarán los cambios significativos de política cuando se produzcan para asegurar su idoneidad, adecuación y efectividad continuas.	BC	SI
6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION				
6.1	ORGANIZACIÓN INTERNA				
6.1.1	ASIGNACION DE RESPONSABILIDADES PARA LA SEG DE LA INFORMACION	Todas las responsabilidades de seguridad de la información serán definidas y asignadas.	Las responsabilidades de seguridad de información corporativa de la compañía están claramente definidas e identificadas en la política indicada.	**BC**	**SI**
6.1.2	SEGREGACION DE TAREAS	Los deberes conflictivos y las áreas de responsabilidad deben ser segregados para reducir las oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la organización.	Existen prácticas específicas para cada uno de estos sistemas en su alcance. Los sistemas privilegiados y los autorizadores tienen un segundo autorizante verificado para evitar oportunidades de uso indebido o abuso. Algunos servicios compartidos utilizan procedimientos especiales para el acceso privilegiado invocado en los sistemas de su entorno.	**BC**	**SI**
6.1.3	CONTACTO CON LAS AUTORIDADES	Se mantendrán contactos apropiados con las autoridades pertinentes.	El contacto con las autoridades pertinentes se mantiene en todos los niveles. Las autoridades pertinentes pueden incluir Departamentos de Gobierno, agencias de aplicación de la ley, servicios de seguridad.	**L BC**	**SI**
6.1.4	CONTACTO CON GRUPOS DE INTERES ESPECIAL	Se mantendrán contactos apropiados con grupos de interés especial u otros foros especializados de seguridad y asociaciones profesionales.	LRQA, ISEB, CBI, BSI, Privacy y organismos nacionales de certificación de la industria.	**BC**	**SI**

6.1.5	**SEGURIDAD DE LA INFORMACION EN LA GESTION DE PROYECTOS**	La seguridad de la información se abordará en la gestión de proyectos, Independientemente del tipo de proyecto.	La compañía ha establecido un equipo de seguridad global. En el nivel de proyecto y de cuenta, se establecerá un Administrador de cuentas de seguridad que relata al ejecutivo de cuentas.	**C BC AR**	**SI**
6.2	**DISPOSITIVOS PARA MOVILIDAD Y TELETRABAJO**				
6.2.1	**POLITICA DE USO DE DISPOSITIVOS PARA MOBILIDAD**	Se adoptará una política y se adoptarán medidas de seguridad de apoyo para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Estándar de seguridad del dispositivo móvil	**BC**	**SI**
6.2.2	**TELETRABAJO**	Se adoptará una política y medidas de seguridad de apoyo para proteger la información accesible, procesada o almacenada en los sitios de teletrabajo.	Estándar de seguridad del dispositivo móvil	**BC**	**SI**
7	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**				
	7.1 **ANTES DE LA CONTRATACION**				
7.1.1	**INVESTIGACION DE ANTECEDENTES**	Verificación de antecedentes de todos los candidatos para el empleo. Se llevará a cabo de conformidad con las leyes y reglamentos pertinentes y la ética y será proporcional a los requisitos de negocio, la clasificación de la información a ser accesible y los riesgos percibidos.	Todos los empleados están sujetos a verificaciones antes del empleo. Algunos roles requieren chequeos adicionales de chequeo nacional, se realiza un "background check".	**L-C BC-AR**	**SI**
7.1.2	**TERMINOS Y CONDICIONES DE CONTRATACION**	Los acuerdos contractuales con empleados y contratistas deberán establecer sus responsabilidades y la de la organización en materia de seguridad de la información.	Los nuevos contratados firman un contrato de trabajo donde se cumplen los requisitos de confidencialidad y no divulgación. Sus obligaciones para la seguridad son las partes de este contrato de empleo. Algunos empleados también completan el examen requerido por los clientes que apoyan (depende de la función, el trabajo realizado y la cuenta particular del cliente apoyado). También según el Contrato de Empleo y los contratos con terceros hay obligación de trabajar y comportarse de acuerdo a todos los requisitos de seguridad.	**L-C BC-AR**	**SI**
7.2	**DURANTE LA CONTRATACION**				

7.2.1	**RESPONSABILIDADES DE GESTION**	La administración requerirá que todos los empleados y contratistas cumplan con la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.	Todos los empleados y contratistas empleados deben cumplir con todos los roles y responsabilidades de seguridad y cualquier violación de dicha seguridad (Política, Procedimientos, Requisitos) puede ser motivo para la terminación. Los usuarios de terceros son tratados como visitantes y sólo tienen acceso de acompañamiento y las infracciones pueden ser causa de eliminación de los privilegios de acceso. También deben respetar todos los roles de seguridad y las responsabilidades del centro.	**L-C BC-AR**	**SI**
7.2.2	**CONCIENCIACION, EDUCACION Y CAPACIDATACION EN SEG. DE LA INF.**	Todos los empleados de la organización y, en su caso, los contratistas recibirán educación y capacitación apropiadas sobre la concienciación y actualizaciones regulares en las políticas y procedimientos de la organización, según sean relevantes para su función laboral.	El entrenamiento de Concientización de Seguridad se da como parte del Proceso de Transferencia de Conocimiento (KT) en el proceso de embarque y también se entrega anualmente. La formación corporativa está vinculada a la organización del CISO.	**C BC-AR**	**SI**
7.2.3	**PROCESO DISCIPLINARIO**	Habrá un proceso disciplinario formal y comunicado para tomar acción contra los empleados que han cometido una violación de la seguridad de la información.	Las acciones disciplinarias formales para los empleados que han cometido una violación de seguridad se utilizan siguiendo las políticas de recursos humanos.	**L-BC**	**SI**
7.3	**CESE O CAMBIO DE PUESTO DE TRABAJO**				
7.3.1	**CESE O CAMBIO DE PUESTO DE TRABAJO**	Las responsabilidades y deberes de seguridad de la información que permanezcan vigentes después de la terminación o cambio de empleo serán definidos, comunicados al empleado o contratista y puestos en vigor.	Las responsabilidades para la terminación del empleo o cambio de empleo serán completadas por Recursos Humanos de acuerdo con las políticas de la compañía.	**C-BC**	**SI**
8	**GESTION DE ACTIVOS**				
8.1	**RESPONSABILIDAD SOBRE LOS ACTIVOS**				
8.1.1	**INVENTARIO DE ACTIVOS**	Se identificarán los activos asociados a instalaciones y se elaborará y mantendrá un inventario de estos activos.	Todos los activos se etiquetan en el punto de recibo. Se mantiene un inventario.	**C-BC-AR**	**SI**

8.1.2	**PROPIEDAD DE LOS ACTIVOS**	Los activos mantenidos en el inventario serán propiedad de la compañía.	Toda la información y los activos del Registro de Activos del SGSI se identifican claramente y se define la propiedad, cada área de negocio tiene un gerente superior claro que es el propietario del activo para su área de negocio. Según la política correspondiente.	**BC**	**SI**
8.1.3	**USO ACEPTABLE DE LOS ACTIVOS**	Las reglas para el uso aceptable de la información y de los activos asociados con las instalaciones y la información deben ser identificadas, documentadas e implementadas.	La compañía sigue declaraciones de uso aceptable en la política correspondiente, y se comunica en sesiones de información anual de seguridad a todos los nuevos entrantes.	**L-C BC-AR**	**SI**
8.1.4	**DEVOLUCION DE LOS ACTIVOS**	Todos los empleados y usuarios de las partes externas devolverán todos los activos de la organización en su poder al finalizar su empleo, contrato o acuerdo.	Todos los empleados y contratistas devuelven todos los activos de la compañía en su posesión al finalizar su empleo, contrato o acuerdo con el Gerente de Recursos Humanos.	**BC-AR**	**SI**
8.2	**CLASIFICACION DE LA INFORMACION**				
8.2.1	**DIRECTRICES DE CLASIFICACION**	La información se clasificará en términos de requisitos legales, valor, criticidad y sensibilidad a la divulgación o modificación no autorizada.	La información se clasifica en términos requeridos según las políticas y directrices de la compañía.	**L-C-BC**	**SI**
8.2.2	**ETIQUETADO Y MANIPILADO DE LA INFORMACION**	Se elaborará y aplicará un conjunto adecuado de procedimientos para el etiquetado de información de conformidad con el esquema de clasificación de información adoptado por la organización.	La información está etiquetada de acuerdo con las políticas, directrices y manejo de información confidencial de la compañía, o de acuerdo con requisitos adicionales especificados por el propietario de la información.	**BC-AR**	**SI**
8.2.3	**MANIPULACION DE ACTIVOS**	Los procedimientos de manipulación de los activos se elaborarán y aplicarán de conformidad con el sistema de clasificación de información adoptado por la organización.	Utilice los medios de comunicación electrónicos que describen cómo manejar, administrar y almacenar los medios electrónicos. Según la política en cuestión.	**BC-AR**	**SI**
8.3	**MANEJO DE LOS SOPORTES DE ALMACENAMIENTO**				
8.3.1	**GESTION DE SOPORTES EXTRAIBLES**	Se aplicarán procedimientos para la gestión de medios amovibles de acuerdo con el esquema de clasificación adoptado por la organización.	Los procedimientos para la gestión de medios extraíbles se detallan en la Guía de seguridad de protección y manipulación de medios removibles de la compañía.	**L-C-BC**	**SI**
8.3.2	**ELIMINACION DE SOPORTES**	Los medios deben ser eliminados de manera segura cuando ya no se requiera, usando procedimientos formales.	Política global de eliminación de la compañía para la eliminación segura de los medios de información.	**L-C-BC**	**SI**

8.3.3	**SOPORTES FISICOS EN TRANSITO**	Los medios que contengan información deberán estar protegidos contra el acceso, uso indebido o corrupción no autorizados durante el transporte.	La política de sanitización y eliminación de la compañía.	**L-C-BC**	**SI**
9	**CONTROL DE ACCESOS**				
9.1	**REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS**				
9.1.1	**POLITICA DE CONTROL DE ACCESOS**	Se establecerá, documentará y revisará una política de control de acceso basada en los requisitos de seguridad de la empresa y la información.	El acceso de usuario de la compañía se debe a un conjunto estándar de privilegios de acceso de acuerdo con la Política de Autorización de Acceso a Datos y Protección de la compañía.	**BC-AR**	**SI**
9.1.2	**CONTORL DE ACCEO A LAS REDES Y SERVICIOS ASOCIADOS**	Los usuarios sólo tendrán acceso a la red y a los servicios de red que hayan sido específicamente autorizados a utilizar.	Se refiere a la política de seguridad correspondiente.	**BC-AR**	**SI**
9.2	**GESTION DE ACCESO DE USUARIO**				
9.2.1	**GESTION DE ALTAS/BAJAS EN EL REGISTRO DE USUARIOS**	Se llevará a cabo un proceso formal de registro y baja de usuarios para permitir la asignación de derechos de acceso.	El formulario y el proceso estándar de petición de la compañía se usan para solicitar el acceso a la compañía estándar para todos los usuarios. Control de acceso estándar.	**C-BC-AR**	**SI**
9.2.2	**GESTION DE LOS DERECJOS DE ACCEOS ASIGNADOS A USUARIOS**	Se implementará un proceso formal de provisión de acceso de usuario para asignar o revocar derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios.	Todo el personal tiene un nombre corto de la compañía que es su identificador único.	**-BC-AR**	**SI**
9.2.3	**GESTION DE LOS DERECHOS DE ACCESO CON PRIVILEGIOS ESPECIALES**	La asignación y el uso de los derechos de acceso privilegiados serán restringidos y controlados.	Las autoridades de la compañía proporcionan derechos de acceso y administran y controlan su asignación, uso y revocación, de acuerdo con las prácticas estándar administradas por los propietarios del sistema.	**-BC-AR**	**SI**
9.2.4	**GESTION DE INFORMACION CONFIDENCIAL DE AUTENTICACION DE USUSARIOS**	La asignación de información de autenticación secreta se controlará mediante un proceso formal de gestión.	Consultar las normas de autenticación y el estándar de control de acceso.	**BC**	**SI**
9.2.5	**REVISION DE LOS DERECHOS DE ACCESO DE LOS USUARIOS**	Los propietarios de activos revisarán los derechos de acceso de los usuarios a intervalos regulares.	Los propietarios de sistemas de la compañía revisan el uso y acceso a sus sistemas.	**BC**	**SI**

9.2.6	**RETIRADO O ADAPTACION DE LOS DERECHOS DE ACCESO**	Los derechos de acceso de todos los empleados y usuarios de las partes externas a las instalaciones de procesamiento de información se eliminarán al terminar su empleo, contrato o acuerdo, o ajustarse al cambio.	Los derechos de acceso de todos los empleados, contratistas y usuarios de terceros a las instalaciones de procesamiento de información serán eliminados al terminar su empleo, el contrato será terminado por Recursos Humanos de acuerdo con las prácticas y políticas de la compañía.	**C-BC**	**SI**
9.3	**RESPONSABILIDADES DEL USUARIO**				
9.3.1	**USO DE INFORMACION CONFIDENCIAL PARA LA AUTENTICACION**	Los usuarios deberán seguir las prácticas de la organización en el uso de la información de autenticación secreta.	Las políticas de contraseñas de la compañía, son aplicadas por el sistema.	**BC**	**SI**
9.4	**CONTROL DE ACCESO A SISTEMAS Y APLICACIONES**				
9.4.1	**RESTRICCION DEL ACCESO A LA INFORMACION**	El acceso a la información y las funciones del sistema de aplicación se restringirán de acuerdo con la política de control de acceso.	La política de autorización y protección de acceso a datos.	**C-BC**	**SI**
9.4.2	**PROCEDIMIENTOS SEGUROS DE INICIO DE SESION**	Cuando así lo exija la política de control de acceso, el acceso a los sistemas y aplicaciones se controlará mediante un procedimiento seguro de conexión.	Se refiere a el estándar de contraseña y autenticación.	**BC**	**SI**
9.4.3	**CUESTION DE CONTRASEÑAS DE USUARIO**	Los sistemas de gestión de contraseñas deben ser interactivos y garantizar contraseñas de calidad.	Contraseña estándar que estipula controles complejos y modificados	**C-BC-AR**	**SI**
9.4.4	**USO DE HERRAMIENTAS DE ADMINISTRACION DE SISTEMAS**	El uso de programas de utilidad que puedan ser capaces de anular los controles del sistema deberán ser restringidos y estrictamente controlados.	Acceso limitado a los administradores de sistemas autorizados.	**BC**	**SI**
9.4.5	**CONTROL DE ACCESO AL CODIGO FUENTE DE LOS PROGRAMAS**	Se restringirá el acceso al código fuente del programa.	Requisito específico de las cuentas.	**C-BC**	**SI**
10	**CIFRADO**				
10.1	**CONTROLES CRIPTOGRAFICOS**				
10.1.1	**POLITICA DE USO DE LOS CONTROLES CRIPTOGRAFICOS**	Se elaborará y aplicará una política sobre el uso de los controles criptográficos para la protección de la información.	Se refiere a la política correspondiente.	**L-C-BC-AR**	**SI**

10.1.2	**GESTION DE CLAVES**	Se desarrollará y aplicará una política sobre el uso, la protección y la duración de las claves criptográficas durante todo su ciclo de vida.	Se refiere a la política correspondiente.	**L-C-BC-AR**	**SI**
11	**SEGURIDAD FISICA Y AMBIENTAL**				
11.1	**AREAS SEGURIDAS**				
11.1.1	**PERIMETRO DE SEGURIDAD FISICA**	Los perímetros de seguridad serán definidos y utilizados para proteger áreas que contengan información sensible o crítica y instalaciones de procesamiento de información.	La compañía utiliza medidas de seguridad física de acuerdo con la política correspondiente.	**C-BC-AR**	**SI**
11.1.2	**CONTROLES FISICOS DE ENTRADA**	Las áreas seguras deben estar protegidas por controles de entrada apropiados para asegurar que sólo el personal autorizado tenga acceso	La compañía utiliza medidas de seguridad física de acuerdo con la política correspondiente.	**C-BC-AR**	**SI**
11.1.3	**SEGURIDAD DE OFICINAS, DESPACHOS Y RECURSOS**	Se diseñará y aplicará la seguridad física de las oficinas, habitaciones e instalaciones.	La compañía utiliza medidas de seguridad física de acuerdo con la política correspondiente.	**C-BC-AR**	**SI**
11.1.4	**PROTECCION CONTRA LAS AMENAZAS EXTERNAS Y AMBIENTALES**	Se diseñará y aplicará protección física contra desastres naturales, ataques maliciosos o accidentes.	Todos los sitios están sujetos a evaluación de riesgos antes y durante la ocupación	**C-BC-AR**	**SI**
11.1.5	**EL TRABAJO EN AREAS SEGURAS**	Se diseñarán y aplicarán procedimientos para trabajar en áreas seguras.	La compañía utiliza medidas de seguridad física de acuerdo con la política correspondiente.	**C-BC-AR**	**SI**
11.1.6	**AREAS DE ACCESO PUBLICO, CARGA Y DESCARGA**	Los puntos de acceso, tales como zonas de entrega y de carga y otros puntos en los que personas no autorizadas puedan entrar en los locales, deberán ser controlados y, si es posible, aislados de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	La compañía utiliza medidas de seguridad física de acuerdo con la política correspondiente.	**C-BC-AR**	**SI**
11.2	**SEGURIDAD DE LOS EQUIPOS**				
11.2.1	**EMPLAZAMIENTO Y PROTECCION DE EQUIPOS**	El equipo estará situado y protegido para reducir los riesgos de amenazas y peligros ambientales y las oportunidades de acceso no autorizado.	Todos los sitios están sujetos a evaluaciones de riesgo antes y durante la ocupación	**C-BC-AR**	**SI**
11.2.2	**INSTALACIONES DE SUMINISTRO**	El equipo debe estar protegido contra fallas de alimentación y otras interrupciones causadas por fallas en las utilidades de apoyo.	Todo el equipo crítico está protegido por UPS y el generador diésel autónomo.	**C-BC-AR**	**SI**

11.2.3	**SEGURIDAD DEL CABLEADO**	Los cables de alimentación y telecomunicaciones que transporten datos o servicios de información de apoyo deberán estar protegidos contra intercepciones, interferencias o daños.	Los cables de alimentación y telecomunicaciones que transportan datos o servicios de información de apoyo están protegidos en salas de datos dentro de los bastidores de cableado. El cableado se inspecciona y se evalúa en las evaluaciones de riesgo de los centros de datos y de entrega. Las normas corporativas para el cifrado de sucursales son utilizadas.	**C-BC**	**SI**
11.2.4	**MANTENIMIENTO DE LOS EQUIPOS**	El equipo se mantendrá correctamente para asegurar su disponibilidad e integridad.	El Administrador de TI cuida de los equipos del centro.	**BC-AR**	**SI**
11.2.5	**SALIDA DE ACTIVOS FUERA DE LAS DEPENDENCIAS DE LA EMPRESA**	El equipo, la información o el software no se deben sacar fuera del sitio sin autorización previa.	Estos son aprobados por el Director o Gerente del Centro. Se permite a los usuarios que los portátiles sean sacados de la instalación bajo previa autorización.	**L-C-BC**	**SI**
11.2.6	**SEGURIDAD DE LOS EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES**	La seguridad se aplicará a los activos fuera del emplazamiento teniendo en cuenta los diferentes riesgos de trabajar fuera de los locales de la organización.	Aunque en virtud del alcance específico de este SoA, no todos los entornos hospedados externos incluidos los entornos de Recuperación ante un Desastre, ya que son específicos del cliente, no están sujetos a este control. La mayoría de los centros críticos y cruciales no requieren la colocación de activos críticos fuera de dicho centro.	**C-BC**	**SI**
11.2.7	**REUTILIZACION O RETIRADA SEGURDA DE DISPOSITIVOS DE ALMACENAMIENTO**	Todos los equipos que contengan medios de almacenamiento deberán ser verificados para asegurar que los datos sensibles y el software con licencia hayan sido removidos o sobrescritos de forma segura antes de su eliminación o reutilización.	Todos los equipos que contienen medios de almacenamiento se comprueban para asegurarse de que los datos confidenciales y el software con licencia se han eliminado y sobrescritos de forma segura (utilizando herramientas aprobadas) antes de su eliminación o reutilización. Si se necesita equipo para transferir al proveedor, se eliminará todo el medio de almacenamiento antes de transferirlo.	**C-BC-AR**	**SI**
11.2.8	**EQUIPO INFORMATICO DE USUARIO DESATENDIDO**	Los usuarios deberán asegurarse de que el equipo desatendido cuente con la protección adecuada.	Bloquear la pantalla por el usuario al dejar desatendido el ordenador.	**L-C-BC-AR**	**SI**

11.2.9	**POLITICA DE PUESTO DE TRABAJO DESPEJADO Y BLOQUEO DE PANTALLA**	Se adoptará una política de escritorio limpio para papeles y medios de almacenamiento extraíbles y una política de pantalla limpia para instalaciones de procesamiento de información.	El bloqueo de pantalla y la política de escritorio limpio se mantienen en toda la compañía.	**C-BC-AR**	**SI**
12	**SEGURIDAD EN LA OPERATIVA**				
12.1	**RESPONSABILIDADES Y PROCEDIMIENTO DE OPERACION**				
12.1.1	**DOCUMENTACION DE PROCEDIMIENTO DE OPERACION**	Los procedimientos operativos deberán documentarse y ponerse a disposición de todos los usuarios que los necesiten.	Los procedimientos operativos se almacenan en los repositorios oficiales del centro.	**BC**	**SI**
12.1.2	**GESTION DE CAMBIOS**	Deben controlarse los cambios en la organización, los procesos empresariales, las instalaciones de procesamiento de información y los sistemas que afectan a la seguridad de la información.	Todos los cambios en los entornos están controlados por "Global Configuration Access Requests Stasytem (GCARS)"	**C-BC-AR**	**SI**
12.1.3	**GESTION DE CAPACIDADES**	El uso de los recursos será monitoreado, para asegurar el desempeño requerido del sistema.	Se llevan a cabo tareas de gestión de capacidad y aprobaciones para sus entornos utilizando procesos estandarizados sujetos a las aprobaciones de GCARS.	**BC**	**SI**
12.1.4	**SEPARACION DE ENTORNOS DE DESARROLLO, PRUEBA Y PRODUCCION**	Los entornos de desarrollo, pruebas y operacionales deben estar separados para reducir los riesgos de acceso no autorizado o cambios en el entorno operacional.	Todos los entornos de Desarrollo, Prueba y Producción se separan físicamente o lógicamente usando switches y firewalls.	**BC**	**SI**
12.2	**PROTECCION CONTRA CODIGO MALICIOSO**				
12.2.1	**CONTROLES CONTRA EL CODIGO MALICIOSO**	Se implementarán controles de detección, prevención y recuperación como protección contra el malware, combinados con una correcta concienciación del usuario.	La compañía utiliza McAfee Antivirus para la detección, prevención. Y controles de recuperación para proteger contra código malicioso	**BC-AR**	**SI**
12.3	**COPIAS DE SEGURIDAD**				
12.3.1	**COPIAS DE SEGURIDAD DE LA INFORMACION**	Copias de seguridad de información, software e imágenes del sistema deben ser tomadas y probadas regularmente de acuerdo con una política de respaldo acordada.	Según la política existente.	**C-BC**	**SI**
12.4	**REGISTRO DE ACTIVIDAD Y SUPERVISION**				

12.4.1	**REGISTRO Y GESTION DE EVENTOS DE ACTIVIDAD**	Los registros de eventos que registran las actividades del usuario, las excepciones, los fallos y los eventos de seguridad de la información se deben mantener y revisar periódicamente.	Se refiere a la política de registro de seguridad.	**C-BC**	**SI**
12.4.2	**PROTECCION DE LOS REGISTROS DE INFORMACION**	Las instalaciones y la información deberán estar protegidas contra la manipulación indebida y el acceso no autorizado.	Los registros de auditoría se conservarán en un área central segura.	**BC**	**SI**
12.4.3	**REGISTROS DE ACTIVIDAD DEL ADMINISTRADOR Y OPERADOR DEL SISTEMA**	Las actividades del administrador del sistema y del operador del sistema se registrarán y los registros se protegerán y se revisarán periódicamente.	Se refiere a política de registro de seguridad se refiere	**C-BC**	**SI**
12.4.4	**SINCRONIZACION DE RELOJES**	Los relojes de todos los sistemas de procesamiento de información relevantes dentro de una organización o dominio de seguridad se sincronizarán con una única fuente de tiempo de referencia.	Todos los sistemas se sincronizarán con un reloj identificado y se mostrarán en GMT. Una lista de relojes disponibles está en la sección 11 de la política correspondiente.	**BC**	**SI**
12.5	**CONTROL DE SOFTWARE EN EXPLOTACION**				
12.5.1	**INSTALACION DEL SOFTWARE EN SISTEMAS EN PRODUCCION**	Se implementarán procedimientos para controlar la instalación de software en sistemas operativos.	La Política de seguridad del sistema operativo prohíbe la instalación de software no aprobado.	**L-C-BC-AR**	**SI**
12.6	**GESTION DE LA VULNERABILIDAD TECNICA**				
12.6.1	**GESTION DE LAS VULNERABILIDADES TECNICAS**	La información sobre las vulnerabilidades técnicas de los sistemas de información que se utilicen se obtendrá oportunamente, se evaluará la exposición de la organización a dichas vulnerabilidades y se tomarán las medidas apropiadas para abordar el riesgo asociado.	Las redes se monitorizan por los centros de operaciones de seguridad.	**BC**	**SI**
12.6.2	**RESTRICCIONES EN LA INSTALACION DE SOFTWARE**	Se establecerán e implementarán las reglas que rijan la instalación de software por parte de los usuarios.	Entorno operativo estándar según la política correspondiente prohíbe la instalación de software por parte de los usuarios.	**BC**	**SI**
12.7	**CONSIDERACIONES DE LAS AUDITORIAS DE LOS SISTEMAS DE INFORMACION**				
12.7.1	**CONTROLES DE AUDITORIA DE LOS SISTEMAS DE INFORMACION**	Los requisitos de auditoría y las actividades que impliquen la verificación de los sistemas operativos se planearán y acordarán cuidadosamente para minimizar las interrupciones en los procesos empresariales.	El responsable global del SGSI mantiene un programa de auditoría	**BC-AR**	**SI**
13	**SEGURIDAD EN LAS TELECOMUNICACIONES**				

13.1	**GESTION DE LA SEGURIDAD EN LAS REDES**				
13.1.1	**CONTROLES DE RED**	Las redes serán gestionadas y controladas para proteger la información en sistemas y aplicaciones.	Las redes serán gestionadas y controladas para proteger la información en sistemas y aplicaciones.	**C-BC**	**SI**
13.1.2	**MECANISMOS DE SEGURIDAD ASOCIADOS A SERVICIOS EN RED**	Los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red se identificarán e incluirán en los acuerdos de servicios de red, ya se trate de servicios internos.	Servicios de red de la compañía realizados y entregados por MNS, CGEN o ciberseguridad.	**BC**	**SI**
13.1.3	**SEGREGACION DE REDES**	Los grupos de servicios de información, usuarios y sistemas de información se segregarán en redes.	Se refiere a la política de Arquitectura de Red	**C-BC**	**SI**
13.2	**INTERCAMBIO DE INFORMACION CON PARTES EXTERNAS**				
13.2.1	**POLITICAS Y PROCEDIMIENTOS DE INTERCAMBIO DE INFORMACION**	Se establecerán políticas, procedimientos y controles de transferencia formal para proteger la transferencia de información mediante el uso de todo tipo de medios de comunicación.	La compañía sigue un proceso documentado formal - Autorización de acceso a datos y política de gestión de protección.	**BC-AR**	**SI**
13.2.2	**ACERDOS DE INTERCAMBIO**	Los acuerdos deberán abordar la transferencia segura de información comercial entre la organización y las partes externas.	La política de conectividad de terceros de la compañía.	**C-BR**	**SI**
13.2.3	**MENSAJERIA ELECTRONICA**	La información involucrada en la mensajería electrónica deberá estar debidamente protegida.	Se refiere a la política en concreto.	**C-BR**	**SI**
13.2.4	**ACUERDOS DE CONFIDENCIALIDAD Y SECRETO**	Los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información se identificarán, revisarán y documentarán periódicamente.	Los acuerdos de confidencialidad y las cláusulas de confidencialidad se incluyen en los contratos de trabajo. Las terceras partes están sujetas a cláusulas de confidencialidad dentro de los contratos, según la política.	**L-C-BC-AR**	**SI**
14	**ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION**				
14.1	**REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACION**				
14.1.1	**ANALISIS Y ESPECIFICACION DE LOS REQUISITOS DE SEGURIDAD**	Los requisitos relacionados con la seguridad de la información se incluirán en los requisitos para nuevos sistemas de información o mejoras en los sistemas de información existentes.	Todas las nuevas peticiones y cambios del sistema son revisadas por las juntas de control de configuración y controladas por el proceso especifico.	**C-BC**	**SI**

14.1.2	**SEGURIDAD DE LAS COMUNICACIONES EN SERVICIOS ACCESIBLES POR REDES PUBLICAS**	La información relacionada con los servicios de aplicación que pasen por las redes públicas estará protegida contra actividades fraudulentas, conflictos contractuales y divulgación y modificación no autorizadas.	Los centros de datos son SSAE 16 / ISAE 3402 auditados según lo requieran las cuentas alojadas	**L-C-BC**	**SI**
14.1.3	**PROTECCION DE LAS TRANSACCIONES POR REDES TELEMATICAS**	La información involucrada en las transacciones del servicio de aplicación estará protegida para evitar la transmisión incompleta, el enrutamiento erróneo, la alteración no autorizada del mensaje, la divulgación no autorizada, la duplicación no autorizada de mensajes o la repetición.	Los centros de datos son SSAE 16 / ISAE 3402 auditados según lo requieran las cuentas alojadas	**BC**	**SI**
14.2	**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE**				
14.2.1	**POLITICA DE DESARROLLO DE SOFTWARE**	Las normas para el desarrollo de software y sistemas se establecerán y aplicarán a los desarrollos dentro de la organización.	La norma detalla los procesos necesarios para desarrollar software y sistemas	**C-BC**	**SI**
14.2.2	**PROCEDIMIENTOS DE CONTROL DE CAMBIOS EN LOS SISTEMAS**	Los cambios en los sistemas dentro del ciclo de vida del desarrollo se controlarán mediante el uso de procedimientos formales de control de cambios.	Las tarjetas de control de configuración y el proceso GCARS.	**C-BC-AR**	**SI**
14.2.3	**REVISION TECNICA DE LAS APLICACIONES TRAS EFECTUAR CAMBIOS EN EL SISTEMA OPERATIVO**	Cuando se cambian las plataformas operativas, las aplicaciones críticas para el negocio deben ser revisadas y probadas para asegurar que no haya impacto adverso en las operaciones de la organización ni en la seguridad.	Proceso GCARS.	**BC**	**SI**
14.2.4	**RESTRICCIONES A LOS CAMBIOS EN LOS PAQUETES DE SOFTWARE**	Las modificaciones a los paquetes de software deberán ser desalentadas, limitadas a los cambios necesarios y todos los cambios deberán ser estrictamente controlados.	Proceso GCARS.	**C-BC**	**SI**
14.2.5	**USO DE PRINCIPIOS DE INGENIERIA EN PROTECCION DE SISTEMAS**	Los principios para la ingeniería de sistemas seguros se establecerán, documentarán, se mantendrán y se aplicarán a cualquier esfuerzo de implementación del sistema de información.	La compañía mantiene un conjunto de políticas, procedimientos y directrices para garantizar soluciones de ingeniería seguras.	**BC**	**SI**
14.2.6	**SEGURIDAD EN ENTORNOS DE DESARROLLO**	Las organizaciones deben establecer y proteger apropiadamente entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida del desarrollo del sistema.	Todos los sistemas de prueba y desarrollo están separados (físicamente o lógicamente) de entornos de producción	**BC**	**SI**

14.2.7	**EXTERNALIZACION DEL DESARROLLO DE SOFTWARE**	Las organizaciones deben establecer y proteger apropiadamente entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida del desarrollo del sistema.	Acuerdo de confidencialidad.	**BC**	**SI**
14.2.8	**PRUEBAS DE FUNCIONALIDAD DURANTE EL DESARROLLO DE LOS SISTEMAS**	Las pruebas de la funcionalidad de seguridad se llevarán a cabo durante el desarrollo	Todos los sistemas están sujetos a pruebas internas y pruebas de aceptación antes del despliegue	**C-BC**	**SI**
14.2.9	**PRUEBAS DE ACEPTACION**	Se establecerán programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.	Los procesos de gestión de la compañía y las aprobaciones de GCARS.	**BC**	**SI**
14.3	**DATOS DE PRUEBA**				
14.3.1	**PROTECCION DE LOS DATOS UTILIZADOS EN PRUEBAS**	Los datos de la prueba se seleccionarán cuidadosamente, se protegerán y se controlarán.	Requisito específico.	**BC**	**SI**
15	**RELACIONES CON SUMINISTRADORES**				
15.1	**SEGURIDAD DE LA INFORMACION EN LAS RELACIONES CON SUMINISTRADORES**				
15.1.1	**POLITICA DE SEG. DE LA INFORMACION PARA SUMINISTRADORES**	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso del proveedor a los activos de la organización se acordarán con el proveedor y se documentarán.	Esta información se mantiene en contratos de terceros	**C-BC-AR**	**SI**
15.1.2	**TRATAMIENTO DEL RIESGO DENTRO DE ACUERDOS DE SUMINISTRADORES**	Todos los requisitos pertinentes de seguridad de la información deberán establecerse y acordarse con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización.	Los contratos con terceros se realizan de acuerdo a las exigencias de seguridad de CSC. Algunas cuentas pueden requerir un mayor control que los controles de seguridad estándar de la compañía. Los controles adicionales se detallan anexos.	**C**	**SI**
15.1.3	**CADENA DE SUMINISTRO EN TECNOLOGIAS DE LA INF. Y CONMUNICACIONES**	Los acuerdos con proveedores incluirán requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	La compañía utiliza un sistema de contrato que incluye requisitos de seguridad.	**C**	**SI**
15.2	**GESTION DE LA PRESTACION DEL SERVICIO POR SUMINISTRADORES**				

15.2.1	**SUPERVISION Y REVISION DE LOS SERVICIOS PRESTADOS POR TERCEROS**	Las organizaciones supervisarán y revisarán periódicamente la prestación de servicios de los proveedores.	La compañía monitorea regularmente o realiza revisiones y auditorías de servicios proporcionados por terceros a su Centro, instalación y operaciones.	**C**	**SI**
15.2.2	**GESTION DE CAMBIOS EN LOS SERVICIOS PRESTADOS POR TERCEROS**	Los cambios en la prestación de servicios, incluido el mantenimiento y mejora de las políticas, procedimientos y controles de seguridad de la información existentes, se gestionarán teniendo en cuenta la criticidad de los sistemas y procesos empresariales implicados y la reevaluación de los riesgos.	Según la política.	**C-BC**	**SI**
16	**GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION**				
16.1	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION Y MEJORAS**				
16.1.1	**RESPONSABILIDADES Y PROCEDIMIENTOS**	Se establecerán responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	La SIRCC coordina todas las respuestas de seguridad	**C-BC-AR**	**SI**
16.1.2	**NOTIFICACION DE LOS EVENTOS DE SEGURIDAD DE LA INFORMACION**	Se establecerán responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	La SIRCC coordina todas las respuestas de seguridad	**C-BC-AR**	**SI**
16.1.3	**NOTIFICACION DE PUNTOS DEBILES DE LA SEGURIDAD**	Los empleados y contratistas que utilicen los sistemas y servicios de información de la organización deberán tomar nota y reportar cualquier debilidad observada o sospechosa de seguridad de información en sistemas o servicios.	Los empleados y contratistas son informados sobre los procedimientos de seguridad instruidos para informar cualquier debilidad de seguridad observada o sospechada en sistemas o servicios para la administración y toda la seguridad.	**BC**	**SI**
16.1.4	**VALORACION DE EVENTOS DE SEG. DE LA INF. Y TOMA DE DECISIONES**	Se evaluarán los eventos de seguridad de la información y se decidirá si deben clasificarse como incidentes de seguridad de la información.	La gestión de informes y la norma de investigación identifica qué eventos se consideran incidentes.	**BC**	**SI**
16.1.5	**RESPUESTA A LOS INDICES DE SEGURIDAD**	Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	La compañía tiene un procedimiento documentado de gestión de incidentes de seguridad.	**C-BC**	**SI**
16.1.6	**APRENDIZAJE DE LOS INCIDENTES DE SEG. DE LA INFORMACION**	Se utilizará el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la probabilidad o el impacto de futuros incidentes.	SIRCC mantiene registros de incidentes	**BC**	**SI**

16.1.7	**RECOPILACION DE EVIDENCIAS**	La organización definirá y aplicará procedimientos para la identificación, recopilación, adquisición y conservación de la información, que pueden servir como prueba.	El manager de seguridad de la compañía mantiene una cadena de custodia de evidencia relacionada con la seguridad.	**C-BC**	**SI**
17	**ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DEL NEGOCIO**				
17.1	**CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION**				
17.1.1	**PLANIFICACION DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION**	La organización determinará sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o un desastre.	Según la política.	**BC-AR**	**SI**
17.1.2	**IMPLANTACION DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION**	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad para la seguridad de la información durante una situación adversa.	Según la política.	**BC**	**SI**
17.1.3	**VERIFICACION, REVISION Y EVALUACION DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION.**	La organización verificará los controles de continuidad de la seguridad de la información establecidos e implementados a intervalos regulares para asegurar que sean válidos y eficaces durante situaciones adversas.	Según la política.	**BC**	**SI**
17.2	**REDUNDANCIAS**				
17.2.1	**DISPONIBILIDAD DE INSTALACIONES PARA EL PROCESAMIENTO DE LA INFORMACION**	Las instalaciones de tratamiento de la información se ejecutarán con una redundancia suficiente para satisfacer los requisitos de disponibilidad.	La compañía proporciona redundancia del sistema según lo solicitado por los clientes sujetos a requisitos contractuales	**C-BC**	**SI**
18	**CUMPLIMIENTO**				
18.1	**CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES**				
18.1.1	**IDENTIFICACION DE LA LEGISLACION APLICABLE**	Todos los requisitos legislativos, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplir con estos requisitos deberán identificarse explícitamente, documentarse y mantenerse al día para cada sistema de información y la organización.	Las políticas identifican requisitos legales.	**C-BC**	**SI**

18.1.2	**DERECHOS DE PROPIEDAD INTELECTUAL(DPI)**	Se aplicarán todos los requisitos legislativos, reglamentarios y contractuales pertinentes y los procedimientos apropiados para garantizar el cumplimiento de los requisitos legislativos, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	Contrato de trabajo con las clausulas pertinentes.	**C-BC**	**SI**
18.1.3	**PROTECCION DE LOS REGISTROS DE LA ORGANIZACIÓN**	Los registros estarán protegidos contra la pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de conformidad con los requisitos legislativos, reglamentarios, contractuales y comerciales	Según la política de retención de registros.	**BC**	**SI**
18.1.4	**PROTECCION DE DATOS Y PRIVACIDAD DE LA INF. PERSONAL**	La privacidad y la protección de la información de identificación personal se garantizará según se requiera en la legislación y la reglamentación pertinentes cuando proceda.	Según la política	**L-C-BC**	**SI**
18.1.5	**REGULACION DE LOS CONTORLES CRIPTOGRAFICOS**	Los controles criptográficos se utilizarán de conformidad con todos los acuerdos, leyes y reglamentos pertinentes.	Según la política	**L-C-BC-AR**	**SI**
18.2	**REVISIONES DE LA SEGURIDAD DE LA INFORMACION**				
18.2.1	**REVISION INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACION**	El enfoque de la organización para gestionar la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para la seguridad de la información) se revisarán independientemente a intervalos planificados o cuando se produzcan cambios significativos.	Las políticas y los procedimientos se revisan anualmente o cuando ocurre un cambio significativo.	**BC**	**SI**
18.2.2	**CUMPLIMIENTO DE LAS POLITICAS Y NORMAS DE SEGURIDAD**	Los administradores revisarán periódicamente el cumplimiento del proceso de información y los procedimientos dentro de su área de responsabilidad con las políticas de seguridad, estándares y cualquier otro requisito de seguridad.	Revisión anual de Políticas y procedimientos complementados con capacitación de Sensibilización a la Seguridad	**BC**	**SI**
18.2.3	**COMPROBACION DEL CUMPLIMIENTO**	Los sistemas de información se revisarán periódicamente para verificar el cumplimiento de las políticas y normas de seguridad de la información de la organización.	Las evaluaciones basadas en herramientas de vulnerabilidad son realizadas por GNS.	**BC-AR**	**SI**

Tabla 3: Declaración de aplicabilidad

- **Metodología de análisis de riesgos.**

Toda organización que planee certificarse en ISO 27001 deberá de llevar a cabo un análisis de riesgos sobre su sistema para determinar que activos están en riesgo. Se debe tomar la decisión en relación a que riesgos la organización aceptara y que controles serán implantados para mitigar el riesgo. Se requiere que la dirección revise la gestión de riesgos para evaluar los niveles de riesgo aceptados y el estado del riesgo residual.
La metodología que se utilizará en el análisis de riesgos será Magerit v3.0. Es una metodología muy extendida, que tiene la ventaja de expresar sus resultados en términos cuantitativos, es decir, en valores económicos. Esto facilita la toma decisiones y su validación por dirección.

Las fases de esta metodología serán:

- Identificación de activos: realizar una identificación, valoración de los activos, que serán los elementos a proteger.
- Valoración de los activos: cada uno de los activos debe tener su valoración.
- Identificación de amenazas: Identificar y valorar las amenazas a las que se encuentran expuestos estos activos. Los activos están sujetos a muchos tipos de amenaza y estas son capaces de causar un incidente en el que el sistema, la organización o los activos pueden resultar dañados.
- Calculo del impacto: se calculará el impacto, que no es más que la cuantificación del daño que se puede producir sobre el activo al producirse la amenaza.

Impacto = Valor del activo x Porcentaje de impacto

- Calculo del riesgo: Una vez que se ha calculado el impacto potencial se puede calcular el riesgo potencial asociado teniendo en cuenta la frecuencia con la que puede tener lugar.

Riesgo = Frecuencia x Impacto

- Selección apropiada de tratamiento: cuando los riesgos se han identificado, deben evaluarse las acciones más apropiadas para llevar a cabo.
- Reducción del riesgo y riesgos residual: en los riesgos que se han decidido tratar se ha reducido el riesgo en una cantidad “X” quedando normalmente un riesgo menor a la inicial, al cual se denomina riesgo residual.

A continuación, establecemos algunos de los criterios que serán usados para las diferentes valoraciones de los activos y los cálculos necesarios.

En la primera tabla de todas podemos ver una valoración económica en función de los diferentes niveles.

		DEFINICION - NIVELES - VULNERABILIDADES
NIVEL	RANGO	DEFINICION
Muy alto (MA)	>100 MIL€	La pérdida o indisponibilidad del activo resultaría catastrófico para la compañía.
Alto(A)	40 MIL € <VALOR<100MILL €	La pérdida o indisponibilidad del activo afecta considerablemente a la compañía.
Medio(M)	5 MIL€ < VALOR < 40 MIL €	La pérdida o indisponibilidad del activo afecta levemente a la compañía.
Bajo(B)	MIL € < VALOR < 5 MIL €	La pérdida o indisponibilidad del activo afecta imperceptiblemente a la compañía.
Muy bajo(MB)	< MIL €	La pérdida o indisponibilidad del activo apenas afecta a la compañía.

Tabla 4: Valoración cualitativa de activos

En la segunda tabla vemos una valoracion cualitativa en funcion de un valor numerico y la gravedad del daño.

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

Tabla 5: Valoración de activos

En la tercera se define una tabla en la cual se reflejarán las frecuencias con la que se pueden dar las amenazas para cada activo. Los rangos máximos y mínimos escogidos han sido de 1 año y 1 días respectivamente.

FRECUENCIA	RANGO	VALOR
Frecuencia muy alta [FMA]	Una vez al día	100
Frecuencia alta [FA]	Una vez al mes	10
Frecuencia media [FM]	Una vez cada trimestre	1
Frecuencia baja [FB]	Una vez cada semestre	0.1
Frecuencia muy baja [FMB]	Una vez al año.	0.01

Tabla 6: Frecuencias y valor asociado

➢ ANALISIS DE RIESGOS:

1. INTRODUCCION:

El primer paso hacia la implementación de un SGSI será la evaluación de los activos realizando una valoración de los mismos.

2. INVENTARIO&VALORACION DE LOS ACTIVOS:

El objetivo final es tomar un conjunto de medidas que garanticen nuestros activos. El sentido comun indica que el coste de las medias no debe ser superior al coste del activo protegido. Se comenzará determinando el valor de los diferentes activos. Asignar esta valoración es realmente complicado en muchos de los casos puesto que puede ser muy subjetiva, no pequeña y con varias copias de seguridad es lo mismo una base de datos de una empresa que la de una gran empresa y sin ningun tipo de control. Esta valoracion se basará en el analisis que propone Magerit en su libro III(punto 2.1), completandolo con una estimacion cuantitativa. La siguiente clasificacion será segun los niveles especificados en la tabla 5.

También se valorarán según sus valores CIA. Se valorará cada activo en las distintas dimensiones de seguridad, obteniendo cuál de ellas resulta más crítica para cada activo.

C – **C**onfidencialidad (confidentiality).

I – **I**ntegridad(integrity).

A – **D**isponibilidad (availability).

Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la perdida para la organización si el activo se viera dañado. Para medir cada dimensión se ha utilizado el siguiente criterio extraído de MAGERIT v3.0, libro II, punto 4.

AMBITO	ACTIVO	VALOR	C	I	A
Hardware [HW]	Dispositivos para copias de seguridad	Alto	10	10	8
	Cableado	Alto	8	8	8
	Ordenadores	Medio	8	8	10
	Servidor de archivos	Medio	8	8	10
	Firewalls	Medio	6	8	10
	Dispositivos de almacenamiento	Bajo	8	6	10
	Servidores de internet	Medio	6	6	6
	Servidores de correo	Medio	6	6	6

	Dispositivos móviles	Medio	6	6	8
	Dispositivos de vigilancia	Bajo	6	10	10
	Dispositivos de salida (impresoras, etc. ..)	Bajo	6	6	4
	Servidores de impresión	Bajo	6	10	4
	Routers	Medio	2	8	10
	Switches	Medio	2	9	10
	Dispositivos de telefonía fija	Bajo	2	8	10
	Dispositivos virtuales	Bajo	6	8	10
	Aire acondicionado	Bajo	6	6	6
	UPS	Bajo	6	6	6
Software [SW]	Sistemas operativos	Muy bajo	6	8	10
	Correo electrónico	Alto	10	6	8
	Aplicaciones	Muy bajo	6	8	8
	Herramientas de desarrollo	Muy bajo	6	6	6
	Herramientas administrativas	Muy bajo	6	6	8
Personal [P]	Persona con la autoridad para la toma de decisiones	Alto	2	8	8
	Desarrolladores	Bajo	2	8	6
	Personal de mantenimiento/operaciones	Medio	2	6	6
	Usuarios	Bajo	2	6	6
Infraestructura [INF]	Control de accesos	Bajo	2	8	10
	Comunicaciones	Bajo	2	8	8
	Sistema de refrigeración del edificio	Medio	2	8	10
	CCTV (video vigilancia)	Medio	2	8	8
	Servicios públicos (agua, electricidad, etc…)	Medio	2	8	10
	Instalaciones	Muy bajo	2	8	10
	Habitaciones de comunicaciones	Alto	2	8	10
	Autoridades	Bajo	2	6	6

Organización [ORG]	Políticas de empresa (locales, globales)	Muy bajo	2	8	10
	Procedimientos	Muy bajo	2	8	10
	Estándares	Muy bajo	2	6	6
	Estructura de la organización	Bajo	2	6	6
	Subcontratistas/Proveedores/Fabricantes	Bajo	2	6	10
Información [INF]	Datos de la compañía	Alto	8	8	8
	Datos del cliente	Muy alto	10	8	8
	Información personal	Alto	8	8	8

Tabla 7: Valoración de activos en cuanto a Confidencialidad-Integridad-Disponibilidad

3. ANALISIS DE AMENAZAS:

Los activos están expuestos a amenazas y estas pueden afectar a los distintos aspectos de la seguridad. A nivel metodológico, queremos analizar que amenazas pueden afectar a que activos.

Lo más habitual es construir una tabla inicial de amenazas, en este caso se utilizarán las usadas en la metodología MAGERIT (Libro II, punto 5, "Catálogo de Elementos"). Estas son:

- Desastres naturales.
- De origen industrial.
- Errores y fallos no intencionados.
- Ataques intencionados.

Y con más detalle:

- **[N] Desastres naturales**. Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
  - [N.1] Fuego
  - [N.2] Daños por agua
  - [N.*] Desastres naturales
- [**I] De origen industrial**. Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada. Origen: Natural (accidental):
  - [I.1] Fuego
  - [I.2] Daños por agua
  - [I.*] Desastres industriales.
  - [I.4] Contaminación electromagnética.
  - [I.5] Avería de origen físico o lógico.
  - [I.6] Corte de suministro eléctrico.
  - [I.7] Condiciones inadecuadas de temperatura o humedad
  - [I.8] Fallo de servicios de comunicaciones.
  - [I.9] Interrupción de otros servicios y suministros esenciales
  - [I.10] Degradación de los soportes de almacenamiento de la información.
  - [I.11] Emanaciones electromagnéticas
- **[E] Errores y fallos no intencionados**. Fallos no intencionales causados por las personas. Origen: Humano (accidental)
  - [E.1] Errores de los usuarios

- [E.2] Errores del administrador
- [E.3] Errores de monitorización
- [E.4] Errores de configuración
- [E.8] Difusión de SW dañino
- [E.9] Errores de [re]-encaminamiento
- [E.10] Errores de secuencia
- [E.15] Alteración accidental de la información
- [E.18] Destrucción de la información
- [E.19] Fugas de información
- [E.20] Vulnerabilidades de los programas (SW)
- [E.21] Errores de mantenimiento / actualización de programas (SW)
- [E.23] Errores de mantenimiento / actualización de equipos (HW)
- [E.24] Caída del sistema por agotamiento de recursos
- [E.25] Pérdida de equipos
- [E.28] Indisponibilidad del personal

▪ **[A] Ataques intencionados.** Fallos deliberados causados por las personas. Origen: Humano (deliberado)

- [A.3]Manipulación de los registros de actividad (log)
- [A.4]Manipulación de la configuración
- [A.5]Suplantación de la identidad del usuario
- [A.6]Abuso de privilegios de acceso
- [A.7]Uso no previsto o [A.8]Difusión de software dañino
- [A.9] [Re-]encaminamiento de mensajes
- [A.10]Alteración de secuencia
- [A.11]Acceso no autorizado
- [A.12]Análisis de tráfico
- [A.13]Repudio
- [A.14]Interceptación de información (escucha)
- [A.15]Modificación deliberada de la información
- [A.18]Destrucción de información
- [A.19]Divulgación de información
- [A.22]Manipulación de programas

- [A.23]Manipulación de los equipos
- [A.24]Denegación de servicio
- [A.25]Robo o [A.26]Ataque destructivo
- [A.27]Ocupación enemiga
- [A.28]Indisponibilidad del personal
- [A.29]Extorsión
- [A.30]Ingeniería social (picaresca)

ACTIVO	FREC	C	I	D
HARDWARE				
[HW] - Dispositivos para copias de seguridad	FB	100%	50%	100%
LISTA DE AMENAZAS				
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[I.*] Desastres industriales	FMB			100%
[I.3] Contaminación mecánica	FMB			100%
[I.4] Contaminación electromagnética	FMB			100%
[I.5] Avería de origen físico o lógico	FMB			100%
[I.6] Corte del suministro eléctrico	FB			75%
[I.7] Condiciones inadecuadas de temperatura o humedad	FMB			75%
[E.2] Errores del administrador	FB	50%	50%	50%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FMB			100%
[E.24] Caída del sistema por agotamiento de recursos	FMB			75%
[E.25] Pérdida de equipos	FMB	100%		100%
[A.6] Abuso de privilegios de acceso	FMB	100%	50%	50%
[A.7] Uso no previsto	FB	100%	50%	100%
[A.11] Acceso no autorizado	FMB	50%	50%	100%
[A.23] Manipulación de los equipos	FMB	50%	50%	50%
[A.24] Denegación de servicio	FMB			100%
[A.25] Robo	FMB	100%		100%
[A.26] Ataque destructivo	FMB			100%
[HW] – SERVIDOR DE ARCHIVOS	FM	100%	60%	100%
LISTA DE AMENAZAS				
[N.1] Fuego	FMB			100%

[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[I.*] Desastres industriales	FMB			100%
[I.3] Contaminación mecánica	FMB			100%
[I.4] Contaminación electromagnética	FMB			100%
[I.5] Avería de origen físico o lógico	FMB			100%
[I.6] Corte del suministro eléctrico	FB			75%
[I.7] Condiciones inadecuadas de temperatura o humedad	FMB			75%
[E.2] Errores del administrador	FB	50%	50%	50%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FMB			100%
[E.24] Caída del sistema por agotamiento de recursos	FMB			75%
[E.25] Pérdida de equipos	FMB	100%		100%
[A.6] Abuso de privilegios de acceso	FMB	100%	50%	50%
[A.7] Uso no previsto	FB	100%	50%	100%
[A.11] Acceso no autorizado	FMB	50%	50%	100%
[A.23] Manipulación de los equipos	FMB	50%	50%	50%
[A.24] Denegación de servicio	FMB			100%
[A.25] Robo	FMB	100%		100%
[A.26] Ataque destructivo	FMB			100%
[HW] – SERVIDORES DE INTERNET	FM	100%	60%	100%
LISTA DE AMENAZAS				
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[I.*] Desastres industriales	FMB			100%
[I.3] Contaminación mecánica	FMB			100%

[I.4] Contaminación electromagnética	FMB			100%
[I.5] Avería de origen físico o lógico	FMB			100%
[I.6] Corte del suministro eléctrico	FB			75%
[I.7] Condiciones inadecuadas de temperatura o humedad	FMB			75%
[E.2] Errores del administrador	FB	50%	50%	50%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FMB			100%
[E.24] Caída del sistema por agotamiento de recursos	FMB			75%
[E.25] Pérdida de equipos	FMB	100%		100%
[A.6] Abuso de privilegios de acceso	FMB	100%	50%	50%
[A.7] Uso no previsto	FB	100%	50%	100%
[A.11] Acceso no autorizado	FMB	50%	50%	100%
[A.23] Manipulación de los equipos	FMB	50%	50%	50%
[A.24] Denegación de servicio	FMB			100%
[A.25] Robo	FMB	100%		100%
[A.26] Ataque destructivo	FMB			100%
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[HW] – SERVIDORES DE CORREO	FM	100%	60%	100%
LISTA DE AMENAZAS				
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[I.*] Desastres industriales	FMB			100%
[I.3] Contaminación mecánica	FMB			100%
[I.4] Contaminación electromagnética	FMB			100%

[I.5] Avería de origen físico o lógico	FMB			100%
[I.6] Corte del suministro eléctrico	FB			75%
[I.7] Condiciones inadecuadas de temperatura o humedad	FMB			75%
[E.2] Errores del administrador	FB	50%	50%	50%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FMB			100%
[E.24] Caída del sistema por agotamiento de recursos	FMB			75%
[E.25] Pérdida de equipos	FMB	100%		100%
[A.6] Abuso de privilegios de acceso	FMB	100%	50%	50%
[A.7] Uso no previsto	FB	100%	50%	100%
[A.11] Acceso no autorizado	FMB	50%	50%	100%
[A.23] Manipulación de los equipos	FMB	50%	50%	50%
[A.24] Denegación de servicio	FMB			100%
[A.25] Robo	FMB	100%		100%
[A.26] Ataque destructivo	FMB			100%
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[HW] – SERVIDORES DE IMPRESION	FM	100%	60%	100%
LISTA DE AMENAZAS				
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[I.*] Desastres industriales	FMB			100%
[I.3] Contaminación mecánica	FMB			100%
[I.4] Contaminación electromagnética	FMB			100%
[I.5] Avería de origen físico o lógico	FMB			100%

[I.6] Corte del suministro eléctrico	FB			75%
[I.7] Condiciones inadecuadas de temperatura o humedad	FMB			75%
[E.2] Errores del administrador	FB	50%	50%	50%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FMB			100%
[E.24] Caída del sistema por agotamiento de recursos	FMB			75%
[E.25] Pérdida de equipos	FMB	100%		100%
[A.6] Abuso de privilegios de acceso	FMB	100%	50%	50%
[A.7] Uso no previsto	FB	100%	50%	100%
[A.11] Acceso no autorizado	FMB	50%	50%	100%
[A.23] Manipulación de los equipos	FMB	50%	50%	50%
[A.24] Denegación de servicio	FMB			100%
[A.25] Robo	FMB	100%		100%
[A.26] Ataque destructivo	FMB			100%
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[HW] – CABLEADO	FB	100%	50%	100%
LISTA DE AMENAZAS				
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[I.*] Desastres industriales	FMB			100%
[I.3] Contaminación mecánica	FMB			100%
[I.4] Contaminación electromagnética	FMB			100%
[I.5] Avería de origen físico o lógico	FMB			100%
[I.6] Corte del suministro eléctrico	FMB			100%

[I.7] Condiciones inadecuadas de temperatura o humedad	FMB			100%
[I.9]Interrupción de otros servicios y suministros esenciales	FB			100%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FMB			100%
[E.24] Caída del sistema por agotamiento de recursos	FMB			100%
[E.25] Pérdida de equipos	FMB	10%		40%
[A.6] Abuso de privilegios de acceso	FMB	20%		100%
[A.7] Uso no previsto	FMB	10%	10%	30%
[A.11] Acceso no autorizado	FMB	50%	50%	
[A.23] Manipulación de los equipos	FMB	50%		100%
[A.25] Robo	FMB	100%		100%
[A.26] Ataque destructivo	FMB			100%
[HW] – FIREWALLS	FB	60%	50%	100%
LISTA DE AMENAZAS				
[I.8] Fallo de servicios de comunicaciones.	FMB			50%
[E.2] Errores del administrador	FMB	30	30	50%
[E.9] Errores de encaminamiento	FMB	10		30%
[E.10] Errores de secuencia	FMB		10	50%
[E.15] Alteración accidental de la información	FMB		20	50%
[E.18] Destrucción de información	FMB	30		50%
[E.19] Fugas de información	FMB	30		50%
[E.24] Caída del sistema por agotamiento de recursos	FMB			50%
[A.5] Suplantación de la identidad del usuario	FMB	30		50%
[A.6] Abuso de privilegios de acceso	FMB	30		50%
[A.7]Uso no previsto	FB	30		70%
[A.9] [Re-]encaminamiento de mensajes	FMB			50%
[A.10]Alteración de secuencia	FMB			50%
[A.11]Acceso no autorizado	FMB	50%		50%
[A.12]Análisis de tráfico	FMB	30		50%
[A.14]Interceptación de información (escucha)	FMB	40		50%
[A.15] Modificación deliberada de la información	FMB		40	50%

[A.19] Divulgación de información	FMB	30		50%
[A.24] Denegación de servicio	FMB			80%
[HW] – ROUTERS	FB	60	50	100
LISTA DE AMENAZAS				
[I.8] Fallo de servicios de comunicaciones.	FMB			50%
[E.2] Errores del administrador	FMB	30	30	50%
[E.9] Errores de encaminamiento	FMB	10		30%
[E.10] Errores de secuencia	FMB		10	50%
[E.15] Alteración accidental de la información	FMB		20	50%
[E.18] Destrucción de información	FMB	30		50%
[E.19] Fugas de información	FMB	30		50%
[E.24] Caída del sistema por agotamiento de recursos	FMB			50%
[A.5] Suplantación de la identidad del usuario	FMB	30		50%
[A.6] Abuso de privilegios de acceso	FMB	30		50%
[A.7]Uso no previsto	FB	30		70%
[A.9] [Re-]encaminamiento de mensajes	FMB			50%
[A.10]Alteración de secuencia	FMB			50%
[A.11]Acceso no autorizado	FMB	50%		50%
[A.12]Análisis de tráfico	FMB	30		50%
[A.14]Interceptación de información (escucha)	FMB	40		50%
[A.15] Modificación deliberada de la información	FMB		40	50%
[A.19] Divulgación de información	FMB	30		50%
[A.24] Denegación de servicio	FMB			80%
[HW] – SWITCHES	FB	60	50	100
LISTA DE AMENAZAS				
[I.8] Fallo de servicios de comunicaciones.	FMB			50%
[E.2] Errores del administrador	FMB	30	30	50%
[E.9] Errores de encaminamiento	FMB	10		30%
[E.10] Errores de secuencia	FMB		10	50%
[E.15] Alteración accidental de la información	FMB		20	50%
[E.18] Destrucción de información	FMB	30		50%

[E.19] Fugas de información	FMB	30		50%
[E.24] Caída del sistema por agotamiento de recursos	FMB			50%
[A.5] Suplantación de la identidad del usuario	FMB	30		50%
[A.6] Abuso de privilegios de acceso	FMB	30		50%
[A.7]Uso no previsto	FB	30		70%
[A.9] [Re-]encaminamiento de mensajes	FMB			50%
[A.10]Alteración de secuencia	FMB			50%
[A.11]Acceso no autorizado	FMB	50%		50%
[A.12]Análisis de tráfico	FMB	30		50%
[A.14]Interceptación de información (escucha)	FMB	40		50%
[A.15] Modificación deliberada de la información	FMB		40	50%
[A.19] Divulgación de información	FMB	30		50%
[A.24] Denegación de servicio	FMB			80%
[I.8] Fallo de servicios de comunicaciones.	FMB			50%
[E.2] Errores del administrador	FMB	30	30	50%
[E.9] Errores de encaminamiento	FMB	10		30%
[E.10] Errores de secuencia	FMB		10	50%
[E.15] Alteración accidental de la información	FMB		20	50%
[E.18] Destrucción de información	FMB	30		50%
[E.19] Fugas de información	FMB	30		50%
[E.24] Caída del sistema por agotamiento de recursos	FMB			50%
[HW] – ORDENADORES	FB	100%	50%	100%
LISTA DE AMENAZAS				
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[I.*] Desastres industriales	FMB			100%
[I.3] Contaminación mecánica	FMB			100%

[I.4] Contaminación electromagnética	FMB			100%
[I.5] Avería de origen físico o lógico	FM			100%
[I.6] Corte del suministro eléctrico	FB			100%
[I.7] Condiciones inadecuadas de temperatura o humedad	FB			80%
[E.2] Errores del administrador	FMB	20%	30%	60%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FMB			100%
[E.24] Caída del sistema por agotamiento de recursos	FB			50%
[E.25] Pérdida de equipos	FMB	100%		100%
[A.6] Abuso de privilegios de acceso	FMB	50%		50%
[A.7] Uso no previsto	FMB			100%
[A.11] Acceso no autorizado	FMB	50%	30%	100%
[A.23] Manipulación de los equipos	FMB	30%		30%
[A.24] Denegación de servicio	FMB			100%
[A.25] Robo	FMB	100%		100%
[A.26] Ataque destructivo	FMB			100%
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[HW] – DISPOSITIVOS DE ALMACENAMIENTO	FB	100%	50%	100%
LISTA DE AMENAZAS				
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[I.*] Desastres industriales	FMB			100%
[I.3] Contaminación mecánica	FMB			100%
[I.4] Contaminación electromagnética	FMB			100%

[I.5] Avería de origen físico o lógico	FMB			100%
[I.6] Corte del suministro eléctrico	FB			75%
[I.7] Condiciones inadecuadas de temperatura o humedad	FMB			75%
[E.2] Errores del administrador	FB	50%	50%	50%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FMB			100%
[E.24] Caída del sistema por agotamiento de recursos	FMB			75%
[E.25] Pérdida de equipos	FMB	100%		100%
[A.6] Abuso de privilegios de acceso	FMB	100%	50%	50%
[A.7] Uso no previsto	FB	100%	50%	100%
[A.11] Acceso no autorizado	FMB	50%	50%	100%
[A.23] Manipulación de los equipos	FMB	50%	50%	50%
[A.24] Denegación de servicio	FMB			100%
[A.25] Robo	FMB	100%		100%
[A.26] Ataque destructivo	FMB			100%
[HW] – DISPOSITIVOS MOVILES	FB	100%	50%	100%
LISTA DE AMENAZAS				
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[I.*] Desastres industriales	FMB			100%
[I.3] Contaminación mecánica	FMB			100%
[I.4] Contaminación electromagnética	FMB			100%
[I.5] Avería de origen físico o lógico	FM			100%
[I.6] Corte del suministro eléctrico	FB			100%
[I.7] Condiciones inadecuadas de temperatura o humedad	FB			80%
[E.2] Errores del administrador	FMB	20%	30%	60%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FMB			100%
[E.24] Caída del sistema por agotamiento de recursos	FB			50%

[E.25] Pérdida de equipos	FMB	100%		100%
[A.6] Abuso de privilegios de acceso	FMB	50%		50%
[A.7] Uso no previsto	FMB			100%
[A.11] Acceso no autorizado	FMB	50%	30%	100%
[A.23] Manipulación de los equipos	FMB	30%		30%
[A.24] Denegación de servicio	FMB			100%
[A.25] Robo	FMB	100%		100%
[HW] – DISPOSITIVOS DE VIGILANCIA	FB	50%	50%	100%
LISTA DE AMENAZAS				
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[I.*] Desastres industriales	FMB			100%
[I.3] Contaminación mecánica	FMB			100%
[I.4] Contaminación electromagnética	FMB			100%
[I.5] Avería de origen físico o lógico	FM			100%
[I.6] Corte del suministro eléctrico	FB			100%
[I.7] Condiciones inadecuadas de temperatura o humedad	FB			80%
[E.2] Errores del administrador	FMB	20%	30%	60%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FMB			100%
[E.24] Caída del sistema por agotamiento de recursos	FB			50%
[E.25] Pérdida de equipos	FMB	100%		100%
[A.6] Abuso de privilegios de acceso	FMB	50%		50%
[A.7] Uso no previsto	FMB			100%
[A.11] Acceso no autorizado	FMB	50%	30%	100%
[A.23] Manipulación de los equipos	FMB	30%		30%
[A.24] Denegación de servicio	FMB			100%
[A.25] Robo	FMB	100%		100%

[A.26] Ataque destructivo	FMB			100%
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[HW] – DISPOSITIVOS DE SALIDA (IMPRESORAS, ETC …)	FB	50%	100%	50%
LISTA DE AMENAZAS				
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[I.*] Desastres industriales	FMB			100%
[I.3] Contaminación mecánica	FMB			100%
[I.4] Contaminación electromagnética	FMB			100%
[I.5] Avería de origen físico o lógico	FM			100%
[I.6] Corte del suministro eléctrico	FB			100%
[I.7] Condiciones inadecuadas de temperatura o humedad	FB			80%
[E.2] Errores del administrador	FMB	20%	30%	60%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FMB			100%
[E.24] Caída del sistema por agotamiento de recursos	FB			50%
[E.25] Pérdida de equipos	FMB	100%		100%
[A.6] Abuso de privilegios de acceso	FMB	50%		50%
[A.7] Uso no previsto	FMB			100%
[A.11] Acceso no autorizado	FMB	50%	30%	100%
[A.23] Manipulación de los equipos	FMB	30%		30%
[A.24] Denegación de servicio	FMB			100%
[A.25] Robo	FMB	100%		100%
[A.26] Ataque destructivo	FMB			100%
[N.1] Fuego	FMB			100%

[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[HW] – DISPOSITIVOS DE TELEFONIA FIJA	FB	60	50	100
LISTA DE AMENAZAS				
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[I.*] Desastres industriales	FMB			100%
[I.3] Contaminación mecánica	FMB			100%
[I.4] Contaminación electromagnética	FMB			100%
[I.5] Avería de origen físico o lógico	FM			100%
[I.6] Corte del suministro eléctrico	FB			100%
[I.7] Condiciones inadecuadas de temperatura o humedad	FB			80%
[E.2] Errores del administrador	FMB	20%	30%	60%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FMB			100%
[E.24] Caída del sistema por agotamiento de recursos	FB			50%
[E.25] Pérdida de equipos	FMB	100%		100%
[A.6] Abuso de privilegios de acceso	FMB	50%		50%
[A.7] Uso no previsto	FMB			100%
[A.11] Acceso no autorizado	FMB	50%	30%	100%
[A.23] Manipulación de los equipos	FMB	30%		30%
[A.24] Denegación de servicio	FMB			100%
[A.25] Robo	FMB	100%		100%
[A.26] Ataque destructivo	FMB			100%
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%

[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[HW] – DISPOSITIVOS VIRTUALES	FM	60	50	100
LISTA DE AMENAZAS				
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[I.*] Desastres industriales	FMB			100%
[I.3] Contaminación mecánica	FMB			100%
[I.4] Contaminación electromagnética	FMB			100%
[I.5] Avería de origen físico o lógico	FM			100%
[I.6] Corte del suministro eléctrico	FB			100%
[I.7] Condiciones inadecuadas de temperatura o humedad	FB			80%
[E.2] Errores del administrador	FMB	20%	30%	60%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FMB			100%
[E.24] Caída del sistema por agotamiento de recursos	FB			50%
[E.25] Pérdida de equipos	FMB	100%		100%
[A.6] Abuso de privilegios de acceso	FMB	50%		50%
[A.7] Uso no previsto	FMB			100%
[A.11] Acceso no autorizado	FMB	50%	30%	100%
[A.23] Manipulación de los equipos	FMB	30%		30%
[A.24] Denegación de servicio	FMB			100%
[A.25] Robo	FMB	100%		100%
[A.26] Ataque destructivo	FMB			100%
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FB	10	10	100%

LISTA DE AMENAZAS				
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[I.*] Desastres industriales	FMB			100%
[I.3] Contaminación mecánica	FMB			100%
[I.4] Contaminación electromagnética	FMB			100%
[I.5] Avería de origen físico o lógico	FMB			100%
[I.6] Corte del suministro eléctrico	FMB			100%
[I.7] Condiciones inadecuadas de temperatura o humedad	FMB			100%
[I.9]Interrupción de otros servicios y suministros esenciales	FB			100%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FMB			100%
[E.24] Caída del sistema por agotamiento de recursos	FMB			100%
[E.25] Pérdida de equipos	FMB	10%		40%
[A.6] Abuso de privilegios de acceso	FMB	20%		100%
[A.7] Uso no previsto	FMB	10%	10%	30%
[A.11] Acceso no autorizado	FMB	50%	50%	
[A.23] Manipulación de los equipos	FMB	50%		100%
[A.25] Robo	FMB	100%		100%
[A.26] Ataque destructivo	FMB			100%
[HW] - UPS	FM	50	50	100
LISTA DE AMENAZAS				
[I.8] Fallo de servicios de comunicaciones.	FMB			50%
[E.2] Errores del administrador	FMB	30	30	50%
[E.9] Errores de encaminamiento	FMB	10		30%
[E.10] Errores de secuencia	FMB		10	50%
[E.15] Alteración accidental de la información	FMB		20	50%
[E.18] Destrucción de información	FMB	30		50%
[E.19] Fugas de información	FMB	30		50%

[E.24] Caída del sistema por agotamiento de recursos	FMB			50%
[A.5] Suplantación de la identidad del usuario	FMB	30		50%
[A.6] Abuso de privilegios de acceso	FMB	30		50%
[A.7]Uso no previsto	FB	30		70%
[A.9] [Re-]encaminamiento de mensajes	FMB			50%
[A.10]Alteración de secuencia	FMB			50%
[A.11]Acceso no autorizado	FMB	50%		50%
[A.12]Análisis de tráfico	FMB	30		50%
[A.14]Interceptación de información (escucha)	FMB	40		50%
[A.15] Modificación deliberada de la información	FMB		40	50%
[A.19] Divulgación de información	FMB	30		50%
[A.24] Denegación de servicio	FMB			80%
SOFTWARE				
[SW] – SISTEMAS OPERATIVOS	FA	100	100	100
LISTA DE AMENAZAS				
[i.5] Avería de origen físico o lógico	FB			80
[E.1] Errores de los usuarios	FB	30	30	30
[E.2] Errores del administrador	FMB	40	40	40
[E.8] Difusión de SW dañino	FMB	30	30	50
[E.9] Errores de [re]-encaminamiento	FMB	20		
[E.10] Errores de secuencia	FMB		20	
[E.15] Alteración accidental de la información	FMB		20	
[E.18] Destrucción de la información	FMB			50
[E.19] Fugas de información	FMB	30		
[E.20] Vulnerabilidades de los programas (SW)	FMB	40	40	40
[E.21] Errores de mantenimiento / actualización de programas (SW)	FA		50	50
[A.5]Suplantación de la identidad del usuario	FMB	50	100	
[A.6]Abuso de privilegios de acceso	FMB	40	30	30
[A.7]Uso no previsto o [A.8]Difusión de software dañino	FMB	80	80	100
[A.9] [Re-]encaminamiento de mensajes	FMB	50		
[A.10]Alteración de secuencia	FMB		30	

[A.11]Acceso no autorizado	FMB	50	30	
[A.15]Modificación deliberada de la información	FMB		50	
[A.18]Destrucción de información	FMB			30
[A.19]Divulgación de información	FMB	50		
[A.22]Manipulación de programas	FMB	100	100	100
[SW] – CORREO ELECTRONICO	FA	100	100	100
LISTA DE AMENAZAS				
[i.5] Avería de origen físico o lógico	FB			80
[E.1] Errores de los usuarios	FB	30	30	30
[E.2] Errores del administrador	FMB	40	40	40
[E.8] Difusión de SW dañino	FMB	30	30	50
[E.9] Errores de [re]-encaminamiento	FMB	20		
[E.10] Errores de secuencia	FMB		20	
[E.15] Alteración accidental de la información	FMB		20	
[E.18] Destrucción de la información	FMB			50
[E.19] Fugas de información	FMB	30		
[E.20] Vulnerabilidades de los programas (SW)	FMB	40	40	40
[E.21] Errores de mantenimiento / actualización de programas (SW)	FA		50	50
[A.5]Suplantación de la identidad del usuario	FMB	50	100	
[A.6]Abuso de privilegios de acceso	FMB	40	30	30
[A.7]Uso no previsto o [A.8]Difusión de software dañino	FMB	80	80	100
[A.9] [Re-]encaminamiento de mensajes	FMB	50		
[A.10]Alteración de secuencia	FMB		30	
[A.11]Acceso no autorizado	FMB	50	30	
[A.15]Modificación deliberada de la información	FMB		50	
[A.18]Destrucción de información	FMB			30
[A.19]Divulgación de información	FMB	50		
[A.22]Manipulación de programas	FMB	100	100	100
[SW] - APLICACIONES	FA	100	100	100
LISTA DE AMENAZAS				
[i.5] Avería de origen físico o lógico	FB			80

[E.1] Errores de los usuarios	FB	30	30	30
[E.2] Errores del administrador	FMB	40	40	40
[E.8] Difusión de SW dañino	FMB	30	30	50
[E.9] Errores de [re]-encaminamiento	FMB	20		
[E.10] Errores de secuencia	FMB		20	
[E.15] Alteración accidental de la información	FMB		20	
[E.18] Destrucción de la información	FMB			50
[E.19] Fugas de información	FMB	30		
[E.20] Vulnerabilidades de los programas (SW)	FMB	40	40	40
[E.21] Errores de mantenimiento / actualización de programas (SW)	FA		50	50
[A.5]Suplantación de la identidad del usuario	FMB	50	100	
[A.6]Abuso de privilegios de acceso	FMB	40	30	30
[A.7]Uso no previsto o [A.8]Difusión de software dañino	FMB	80	80	100
[A.9] [Re-]encaminamiento de mensajes	FMB	50		
[A.10]Alteración de secuencia	FMB		30	
[A.11]Acceso no autorizado	FMB	50	30	
[A.15]Modificación deliberada de la información	FMB		50	
[A.18]Destrucción de información	FMB			30
[A.19]Divulgación de información	FMB	50		
[A.22]Manipulación de programas	FMB	100	100	100
[SW] – HERRAMIENTAS DE DESARROLLO	FA	100	100	100
LISTA DE AMENAZAS				
[i.5] Avería de origen físico o lógico	FB			80
[E.1] Errores de los usuarios	FB	30	30	30
[E.2] Errores del administrador	FMB	40	40	40
[E.8] Difusión de SW dañino	FMB	30	30	50
[E.9] Errores de [re]-encaminamiento	FMB	20		
[E.10] Errores de secuencia	FMB		20	
[E.15] Alteración accidental de la información	FMB		20	
[E.18] Destrucción de la información	FMB			50
[E.19] Fugas de información	FMB	30		

[E.20] Vulnerabilidades de los programas (SW)	FMB	40	40	40
[E.21] Errores de mantenimiento / actualización de programas (SW)	FA		50	50
[A.5]Suplantación de la identidad del usuario	FMB	50	100	
[A.6]Abuso de privilegios de acceso	FMB	40	30	30
[A.7]Uso no previsto o [A.8]Difusión de software dañino	FMB	80	80	100
[A.9] [Re-]encaminamiento de mensajes	FMB	50		
[A.10]Alteración de secuencia	FMB		30	
[A.11]Acceso no autorizado	FMB	50	30	
[A.15]Modificación deliberada de la información	FMB		50	
[A.18]Destrucción de información	FMB			30
[A.19]Divulgación de información	FMB	50		
[A.22]Manipulación de programas	FMB	100	100	100
[SW] – HERRAMIENTAS ADMINISTRATIVAS	FA	100	100	100
LISTA DE AMENAZAS				
[i.5] Avería de origen físico o lógico	FB			80
[E.1] Errores de los usuarios	FB	30	30	30
[E.2] Errores del administrador	FMB	40	40	40
[E.8] Difusión de SW dañino	FMB	30	30	50
[E.9] Errores de [re]-encaminamiento	FMB	20		
[E.10] Errores de secuencia	FMB		20	
[E.15] Alteración accidental de la información	FMB		20	
[E.18] Destrucción de la información	FMB			50
[E.19] Fugas de información	FMB	30		
[E.20] Vulnerabilidades de los programas (SW)	FMB	40	40	40
[E.21] Errores de mantenimiento / actualización de programas (SW)	FA		50	50
[A.5]Suplantación de la identidad del usuario	FMB	50	100	
[A.6]Abuso de privilegios de acceso	FMB	40	30	30
[A.7]Uso no previsto o [A.8]Difusión de software dañino	FMB	80	80	100
[A.9] [Re-]encaminamiento de mensajes	FMB	50		
[A.10]Alteración de secuencia	FMB		30	
[A.11]Acceso no autorizado	FMB	50	30	

[A.15]Modificación deliberada de la información	FMB		50	
[A.18]Destrucción de información	FMB			30
[A.19]Divulgación de información	FMB	50		
[A.22]Manipulación de programas	FMB	100	100	100
PERSONAL				
[P] – PERSONA CON LA AUTORIDAD PARA LA TOMA DE DECISIONES	FM	70	50	80
LISTA DE AMENAZAS				
[E.19] Fugas de información	FMB	80		
[E.28] Indisponibilidad del personal	FB			40
[A.28] Indisponibilidad del personal	FMB			60
[A.29] Extorsión	FMB	50	50	50
[A.30] Ingeniería social(picaresca)	FMB	30	30	30
[P] – DESARROLLADORES	FMB	40	20	50
LISTA DE AMENAZAS				
[E.19] Fugas de información	FMB	60		
[E.28] Indisponibilidad del personal	FMB			40
[A.28] Indisponibilidad del personal	FMB			40
[A.29] Extorsión	FMB	60	30	30
[A.30] Ingeniería social(picaresca)	FMB	30	30	30
[P] – PERSONAL DE MANTENIMIENTO - OPERACIONES	FMB	40	20	50
LISTA DE AMENAZAS				
[E.19] Fugas de información	FMB	60		
[E.28] Indisponibilidad del personal	FMB			40
[A.28] Indisponibilidad del personal	FMB			40
[A.29] Extorsión	FMB	60	30	30
[A.30] Ingeniería social(picaresca)	FMB	30	30	30
[P] – USUARIOS	FMB	50	30	50
LISTA DE AMENAZAS				
[E.19] Fugas de información	FMB	60		
[E.28] Indisponibilidad del personal	FMB			40
[A.28] Indisponibilidad del personal	FMB			40
[A.29] Extorsión	FMB	60	30	30

[A.30] Ingeniería social(picaresca)	FMB	30	30	30
INFRAESTRUCTURA				
[INF] – CONTROL DE ACCESOS	FM	20	40	70
LISTA DE AMENAZAS				
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[I.*] Desastres industriales	FMB			100%
[I.3] Contaminación mecánica	FMB			100%
[I.4] Contaminación electromagnética	FMB			100%
[I.5] Avería de origen físico o lógico	FM			100%
[I.6] Corte del suministro eléctrico	FB			100%
[I.7] Condiciones inadecuadas de temperatura o humedad	FB			80%
[E.2] Errores del administrador	FMB	20%	30%	60%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FMB			100%
[E.24] Caída del sistema por agotamiento de recursos	FB			50%
[E.25] Pérdida de equipos	FMB	100%		100%
[A.6] Abuso de privilegios de acceso	FMB	50%		50%
[A.7] Uso no previsto	FMB			100%
[A.11] Acceso no autorizado	FMB	50%	30%	100%
[A.23] Manipulación de los equipos	FMB	30%		30%
[A.24] Denegación de servicio	FMB			100%
[A.25] Robo	FMB	100%		100%
[A.26] Ataque destructivo	FMB			100%
[INF] - COMUNICACIONES	FM	60	50	100
LISTA DE AMENAZAS				
[I.8] Fallo de servicios de comunicaciones.	FMB			50%
[E.2] Errores del administrador	FMB	30	30	50%
[E.9] Errores de encaminamiento	FMB	10		30%

[E.10] Errores de secuencia	FMB		10	50%
[E.15] Alteración accidental de la información	FMB		20	50%
[E.18] Destrucción de información	FMB	30		50%
[E.19] Fugas de información	FMB	30		50%
[E.24] Caída del sistema por agotamiento de recursos	FMB			50%
[A.5] Suplantación de la identidad del usuario	FMB	30		50%
[A.6] Abuso de privilegios de acceso	FMB	30		50%
[A.7]Uso no previsto	FB	30		70%
[A.9] [Re-]encaminamiento de mensajes	FMB			50%
[A.10]Alteración de secuencia	FMB			50%
[A.11]Acceso no autorizado	FMB	50%		50%
[A.12]Análisis de tráfico	FMB	30		50%
[A.14]Interceptación de información (escucha)	FMB	40		50%
[A.15] Modificación deliberada de la información	FMB		40	50%
[A.19] Divulgación de información	FMB	30		50%
[INF] – SISTEMA DE REFRIGERACION DEL EDIFICIO	FB	10	10	100
LISTA DE AMENAZAS				
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[I.*] Desastres industriales	FMB			100%
[I.3] Contaminación mecánica	FMB			100%
[I.4] Contaminación electromagnética	FMB			100%
[I.5] Avería de origen físico o lógico	FMB			100%
[I.6] Corte del suministro eléctrico	FMB			100%
[I.7] Condiciones inadecuadas de temperatura o humedad	FMB			100%
[I.9]Interrupción de otros servicios y suministros esenciales	FB			100%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FMB			100%
[E.24] Caída del sistema por agotamiento de recursos	FMB			100%

[E.25] Pérdida de equipos	FMB	10%		40%
[A.6] Abuso de privilegios de acceso	FMB	20%		100%
[INF] – CCTV(VIDEOVIGILANCIA)	FB	20	20	50
LISTA DE AMENAZAS				
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[I.*] Desastres industriales	FMB			100%
[I.3] Contaminación mecánica	FMB			100%
[I.4] Contaminación electromagnética	FMB			100%
[I.5] Avería de origen físico o lógico	FM			100%
[I.6] Corte del suministro eléctrico	FB			100%
[I.7] Condiciones inadecuadas de temperatura o humedad	FB			80%
[E.2] Errores del administrador	FMB	20%	30%	60%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FMB			100%
[E.24] Caída del sistema por agotamiento de recursos	FB			50%
[E.25] Pérdida de equipos	FMB	100%		100%
[A.6] Abuso de privilegios de acceso	FMB	50%		50%
[A.7] Uso no previsto	FMB			100%
[A.11] Acceso no autorizado	FMB	50%	30%	100%
[A.23] Manipulación de los equipos	FMB	30%		30%
[A.24] Denegación de servicio	FMB			100%
[A.25] Robo	FMB	100%		100%
[A.26] Ataque destructivo	FMB			100%
[A.23] Manipulación de los equipos	FMB	30%		30%
[A.24] Denegación de servicio	FMB			100%
[INF] – SERVICIOS PUBLICOS (AGUA, ELECTRICIDAD, ETC …)	FB	20	20	100
LISTA DE AMENAZAS				
[N.1] Fuego	FMB			100

[N.2] Daños por agua	FMB			100
[N.*] Desastres naturales	FMB			100
[I.1] Fuego	FMB			100
[I.2] Daños por agua	FMB			100
[I.*] Desastres industriales	FMB			100
[E.15] Alteración accidental de la información	FB		25	
[E.18] Destrucción de la información	FMB			50
[E.19] Fugas de información	FMB	20		
[A.7] Uso no previsto	FMB	50	50	50
[A.11]Acceso no autorizado	FMB	50	50	
[A.15]Modificación deliberada de la información	FMB		70	
[A.18]Destrucción de información	FMB			70
[A.19]Divulgación de información	FMB	80		
[A.26] Ataque destructivo	FMB			100
[A.27] ocupación enemiga	FMB	100		100
[INF] - INSTALACIONES	FB	30	30	100
LISTA DE AMENAZAS				
[N.1] Fuego	FMB			100
[N.2] Daños por agua	FMB			100
[N.*] Desastres naturales	FMB			100
[I.1] Fuego	FMB			100
[I.2] Daños por agua	FMB			100
[I.*] Desastres industriales	FMB			100
[E.15] Alteración accidental de la información	FB		25	
[E.18] Destrucción de la información	FMB			50
[E.19] Fugas de información	FMB	20		
[A.7] Uso no previsto	FMB	50	50	50
[A.11]Acceso no autorizado	FMB	50	50	
[A.15]Modificación deliberada de la información	FMB		70	
[A.18]Destrucción de información	FMB			70
[A.19]Divulgación de información	FMB	80		

[A.26] Ataque destructivo	FMB			100
[A.27] ocupación enemiga	FMB	100		100
[INF] – SALAS DE COMUNICACIONES	FA	30	30	100
LISTA DE AMENAZAS				
[N.1] Fuego	FMB			100
[N.2] Daños por agua	FMB			100
[N.*] Desastres naturales	FMB			100
[I.1] Fuego	FMB			100
[I.2] Daños por agua	FMB			100
[I.*] Desastres industriales	FMB			100
[E.15] Alteración accidental de la información	FB		25	
[E.18] Destrucción de la información	FMB			50
[E.19] Fugas de información	FMB	20		
[A.7] Uso no previsto	FMB	50	50	50
[A.11]Acceso no autorizado	FMB	50	50	
ORGANIZACIÓN				
[ORG] - AUTORIDADES	FB	20	20	80
LISTA DE AMENAZAS				
[E.19] Fugas de información	FMB	60		
[E.28] Indisponibilidad del personal	FMB			40
[A.28] Indisponibilidad del personal	FMB			40
[A.29] Extorsión	FMB	60	30	30
[A.30] Ingeniería social(picaresca)	FMB	30	30	30
[ORG] – POLITICAS DE EMPRESA (LOCALES Y GLOBALES)	FB	20	20	100
LISTA DE AMENAZAS				
[E.1] Errores de los usuarios	FB	30	30	30
[E.2] Errores del administrador	FB	40	40	40
[E.15] Alteración accidental de la información	FB		30	
[E.18] Destrucción de información	FB		35	
[E.19] Fugas de información	FB		30	
[A.5] Suplantación de la identidad del usuario	FB	50	30	
[A.6] Abuso de privilegios de acceso	FB	100	50	60

[A.11] Acceso no autorizado	FB	100	50	
[A.15] Modificación deliberada de la información	FB		70	
[A.18] Destrucción de información	FB			100
[A.19] Divulgación de información	FB	100		
[ORG] - PROCEDIMIENTOS	FB	20	20	100
LISTA DE AMENAZAS				
[E.1] Errores de los usuarios	FB	30	30	30
[E.2] Errores del administrador	FB	40	40	40
[E.15] Alteración accidental de la información	FB		30	
[E.18] Destrucción de información	FB		35	
[E.19] Fugas de información	FB		30	
[A.5] Suplantación de la identidad del usuario	FB	50	30	
[A.6] Abuso de privilegios de acceso	FB	100	50	60
[A.11] Acceso no autorizado	FB	100	50	
[A.15] Modificación deliberada de la información	FB		70	
[A.18] Destrucción de información	FB			100
[A.19] Divulgación de información	FB	100		
[ORG] - ESTANDARES	FB	20	20	100
LISTA DE AMENAZAS				
[E.1] Errores de los usuarios	FB	30	30	30
[E.2] Errores del administrador	FB	40	40	40
[E.15] Alteración accidental de la información	FB		30	
[E.18] Destrucción de información	FB		35	
[E.19] Fugas de información	FB		30	
[A.5] Suplantación de la identidad del usuario	FB	50	30	
[A.6] Abuso de privilegios de acceso	FB	100	50	60
[E.1] Errores de los usuarios	FB	30	30	30
[E.2] Errores del administrador	FB	40	40	40
[A.11] Acceso no autorizado	FB	100	50	
[A.15] Modificación deliberada de la información	FB		70	
[A.18] Destrucción de información	FB			100
[A.19] Divulgación de información	FB	100		

[ORG] – SUBCONTRATISTAS-PROVEEDORES-FABRICANTES	FB	20	30	100
LISTA DE AMENAZAS				
[E.1] Errores de los usuarios	FB	30	30	30
[E.2] Errores del administrador	FB	40	40	40
[E.15] Alteración accidental de la información	FB		30	
[E.18] Destrucción de información	FB		35	
[E.19] Fugas de información	FB		30	
[A.5] Suplantación de la identidad del usuario	FB	50	30	
[A.6] Abuso de privilegios de acceso	FB	100	50	60
[E.1] Errores de los usuarios	FB	30	30	30
[E.2] Errores del administrador	FB	40	40	40
[A.11] Acceso no autorizado	FB	100	50	
[A.15] Modificación deliberada de la información	FB		70	
[A.18] Destrucción de información	FB			100
[A.19] Divulgación de información	FB	100		
INFORMACION				
[INF] – DATOS DE LA COMPAÑIA	FA	100	60	60
LISTA DE AMENAZAS				
[E.1] Errores de los usuarios	FA	50	50	50
[E.2] Errores del administrador	FA	50	50	50
[E.15] Alteración accidental de la información	FA	80	80	
[E.18] Destrucción de información	FA	80	30	
[E.19] Fugas de información	FA	80	30	
[A.5] Suplantación de la identidad del usuario	FA	80	80	
[A.6] Abuso de privilegios de acceso	FA	80	80	80
[A.11] Acceso no autorizado	FA	100	50	
[A.15] Modificación deliberada de la información	FA		75	
[A.18] Destrucción de información	FA			100
[A.19] Divulgación de información	FA	100		
[INF] – DATOS DEL CLIENTE	FA	100	60	60
LISTA DE AMENAZAS				
[E.1] Errores de los usuarios	FA	50	50	50

[E.2] Errores del administrador	FA	50	50	50
[E.15] Alteración accidental de la información	FA	80	80	
[E.18] Destrucción de información	FA	80	30	
[E.19] Fugas de información	FA	100	30	
[A.5] Suplantación de la identidad del usuario	FA	100	80	
[A.6] Abuso de privilegios de acceso	FA	100	80	80
[A.11] Acceso no autorizado	FA	100	50	
[A.15] Modificación deliberada de la información	FA		80	
[A.18] Destrucción de información	FA			100
[A.19] Divulgación de información	FA	100		

Tabla 8: Relación entre activos-amenazas

4. IMPACTO:

A continuación, se calculará el impacto, que no es más que la cuantificación del daño que se puede producir sobre el activo al producirse la amenaza.

Impacto = Valor del activo x Porcentaje de impacto

AMBITO	ACTIVO	CRITICIDAD			%IMPACTO			IMP. POTENCIAL		
		C	I	A	C	I	A	C	I	A
Hardware [HW]	Dispositivos para copias de seguridad	10	10	8	100	50	100	10	4	8
	Cableado	8	8	8	100	60	100	8	4.8	8
	Ordenadores	8	8	10	100	60	100	8	4.8	10
	Servidor de archivos	8	8	10	100	60	100	8	4.8	10
	Firewalls	6	8	10	100	60	100	6	4.8	10
	Dispositivos de almacenamiento	8	6	10	100	50	100	8	3	10
	Servidores de internet	6	6	6	60	50	100	3.6	3	6
	Servidores de correo	6	6	6	60	50	100	3.6	3	6
	Dispositivos móviles	6	6	8	60	50	100	3.6	3	8
	Dispositivos de vigilancia	6	10	10	100	50	100	6	5	10
	Dispositivos de salida (impresoras, etc. ..)	6	6	4	100	50	100	6	3	4
	Servidores de impresión	6	10	4	100	50	100	6	5	4
	Routers	2	8	10	50	50	100	1	4	10
	Switches	2	9	10	50	100	50	1	9	5
	Dispositivos de telefonía fija	2	8	10	60	50	100	1.2	4	10
	Dispositivos virtuales	6	8	10	60	50	100	3.6	4	10
	Aire acondicionado	6	6	6	50	50	50	3	3	3
	UPS	8	8	8	50	50	100	4	4	8
Software [SW]	Sistemas operativos	6	8	10	100	100	100	6	8	10
	Correo electrónico	10	6	8	100	100	100	10	6	8

	Aplicaciones	6	8	8	100	100	100	6	8	8
	Herramientas de desarrollo	6	6	6	100	100	100	6	6	6
	Herramientas administrativas	6	6	8	100	100	100	6	6	8
Personal [P]	Persona con la autoridad para la toma de decisiones	2	8	8	70	50	80	1.4	4	6.4
	Desarrolladores	2	8	6	40	20	50	0.8	1.6	3
	Personal de mantenimiento/operaciones	2	6	6	40	20	50	0.8	1.2	3
	Usuarios	2	6	6	50	30	50	1	1.8	3
Infraestructura [INF]	Control de accesos	2	8	10	20	40	70	0.1	3.2	7
	Comunicaciones	2	8	8	60	50	100	1.2	4	8
	Sistema de refrigeración del edificio	2	8	10	10	10	100	0.2	0.8	10
	CCTV (video vigilancia)	2	8	8	20	20	50	0.4	1.6	4
	Servicios públicos (agua, electricidad, etc…)	2	8	10	20	20	50	0.4	1.6	5
	Instalaciones	2	8	10	30	30	100	0.6	2.4	10
	Habitaciones de comunicaciones	2	8	10	30	30	100	0.6	2.4	10
Organización [ORG]	Autoridades	2	6	6	20	20	80	0.4	1.2	4.8
	Políticas de empresa (locales, globales)	2	8	10	20	20	100	0.4	1.6	10
	Procedimientos	2	8	10	20	20	100	0.4	1.6	10
	Estándares	2	6	6	20	20	100	0.4	1.2	6
	Estructura de la organización	2	6	6	20	30	100	0.4	1.8	6
	Subcontratistas/Proveedores/Fabricantes	2	6	10	20	30	100	0.4	1.8	10
Información [INF]	Datos de la compañía	8	8	8	100	60	60	8	4.8	4.8
	Datos del cliente	10	8	8	100	60	60	8	4.8	4.8

Tabla 09: Impacto potencial

5. RIESGO:

Una vez que se ha calculado el impacto potencial se puede calcular el riesgo potencial asociado teniendo en cuenta la frecuencia con la que puede tener lugar, utilizando los límites establecidos en la tabla 6.

Riesgo = Frecuencia x Impacto

AMBITO	ACTIVO	FREC	IMP. POTENCIAL			RIESGO POTENCIAL		
			C	I	A	C	I	A
Hardware [HW]	Dispositivos para copias de seguridad	0.1-FB	10	4	8	1	0.4	0.8
	Cableado	1-FM	8	4.8	8	8	4.8	8
	Ordenadores	1-FM	8	4.8	10	8	4.8	10
	Servidor de archivos	1-FM	8	4.8	10	8	4.8	10
	Firewalls	1-FM	6	4.8	10	6	4.8	10
	Dispositivos de almacenamiento	0.1-FB	8	3	10	0.8	0.3	1
	Servidores de internet	0.1-FB	3.6	3	6	0.36	0.3	0.6
	Servidores de correo	0.1-FB	3.6	3	6	0.36	0.3	0.6
	Dispositivos móviles	0.1-FB	3.6	3	8	0.36	0.3	0.8
	Dispositivos de vigilancia	0.1-FB	6	5	10	0.6	0.5	1
	Dispositivos de salida (impresoras ...)	0.1-FB	6	3	4	0.6	0.3	0.4
	Servidores de impresión	0.1-FB	6	5	4	0.6	0.5	0.4
	Routers	0.1-FB	1	4	10	0.1	0.4	1
	Switches	0.1-FB	1	9	5	0.1	0.9	0.5
	Dispositivos de telefonía fija	0.1-FB	1.2	4	10	0.12	0.4	1
	Dispositivos virtuales	1-FM	3.6	4	10	3.6	4	10
	Aire acondicionado	0.1-FB	3	3	3	0.3	0.3	0.3
	UPS	10-FA	4	4	8	40	40	80
Software [SW]	Sistemas operativos	10-FA	6	8	10	60	80	100
	Correo electrónico	10-FA	10	6	8	100	60	80
	Aplicaciones	10-FA	6	8	8	60	80	80
	Herramientas de desarrollo	10-FA	6	6	6	60	60	60
	Herramientas administrativas	10-FA	6	6	8	60	60	80

Personal [P]	Persona con la autoridad para la toma de decisiones	1-FM	1.4	4	6.4	1.4	4	6.4
	Desarrolladores	0.01-FMB	0.8	1.6	3	0.008	0.016	0.03
	Personal de mantenimiento/operaciones	0.01-FMB	0.8	1.2	3	0.00008	0.012	0.03
	Usuarios	0.01-FMB	1	1.8	3	0.01	0.018	0.03
Infraestructura [INF]	Control de accesos	1-FM	0.1	3.2	7	0.1	3.2	7
	Comunicaciones	1-FM	1.2	4	8	1.2	4	8
	Sistema de refrigeración del edificio	1-FM	0.2	0.8	10	0.2	0.8	10
	CCTV (video vigilancia)	0.1-FB	0.4	1.6	4	0.04	0.16	0.4
	Servicios públicos (agua, electricidad, etc…)	0.1-FB	0.4	1.6	5	0.04	0.16	0.5
	Instalaciones	0.1-FB	0.6	2.4	10	0.06	0.24	1
	Habitaciones de comunicaciones	1-FM	0.6	2.4	10	0.6	2.4	10
Organización [ORG]	Autoridades	0.1-FB	0.4	1.2	4.8	0.04	0.12	0.48
	Políticas de empresa (locales, globales)	0.1-FB	0.4	1.6	10	0.04	0.16	1
	Procedimientos	0.1-FB	0.4	1.6	10	0.04	0.16	1
	Estándares	0.1-FB	0.4	1.2	6	0.04	0.12	0.6
	Estructura de la organización	0.1-FB	0.4	1.8	6	0.04	0.18	0.6
	Subcontratistas/Proveedores/Fabricantes	0.1-FB	0.4	1.8	10	0.04	0.18	1
Información [INF]	Datos de la compañía	10-FA	8	4.8	4.8	80	48	48
	Datos del cliente	10-FA	8	4.8	4.8	80	48	48

Tabla 10: Riesgo potencial

6. RESUMEN:

Una vez finalizada la obtención del riesgo potencial se obtendrán los puntos que se enfrentan a un riesgo mayor por lo que habrá que aplicar medidas que reduzcan este riesgo.
Si el límite de riesgo aceptable ronda, por ejemplo, los 60 puntos obtenemos que fundamentalmente la parte de software y la de información deberá ser revisada para mejorar este nivel de riesgo.

➢ PROPUESTAS DE PROYECTOS:

Introducción:

En el punto anterior se realizó un análisis sobre los activos de la compañía, obteniendo el riesgo potencial asociado a cada activo.

Ahora por tanto en este punto y a partir del riesgo asociado a cada activo se han detectado las áreas más vulnerables, sobre las cuales se trabajará en este apartado para reducir ese riesgo potencial.

Propuesta:

Los proyectos propuestos a continuación ayudarán a reducir el nivel de riesgo potencial que se encuentre por encima del límite estipulado. A continuación, se expondrán los proyectos escogidos y los detalles de cada uno.

- P1 - Salvaguardar la información.
- P2 - Gestión de la información.
- P3 - Actualización de versiones.

PROYECTO 1: SALVAGUARDA DE INFORMACION	
EQUIPO	Responsable de seguridad del centro.
OBJETIVO	Especificar adecuadamente en la política de seguridad existente como se debe de trabajar con información confidencial.
DESCRIPCION	Se refleja en la política de seguridad el trato adecuado que se le debe dar a la información en función del tipo de información que se esté tratando. Se deberá revisar una vez al año para añadir posibles modificaciones.
BENEFICIO	Minimiza la fuga de datos confidenciales
RIESGO A MITIGAR	Información: Datos de la compañía y del cliente. Control: A.5.1
INICIO	15-05-2017
DURACION	2 SEMANAS
FIN	30-05-2017
PRESUPUESTO	300 EUROS
PROYECTO 2: CONTINUIDAD DE NEGOCIO	

EQUIPO	Responsable de seguridad y equipo de mantenimiento (2 personas)
OBJETIVO	Tener un plan definido que asegure la continuidad del negocio en la compañía, en este caso que mantenga la energía eléctrica.
DESCRIPCION	Se evaluará la necesidad de ampliar el número de UPS o la revisión de las existentes.
BENEFICIO	Ante una caída de tensión los usuarios podrás seguir trabajando mientras las UPS alimenten el sistema hasta que salte el generador en caso de existir.
RIESGO A MITIGAR	Hardware: UPS Control: A.17.1 & A17.2
INICIO	30-05-2017
DURACION	3 semanas
FIN	20-06-2017
PRESUPUESTO	1500 euros
PROYECTO 3:DEFINICION DE UNA POLITICA DE ACTUALIZACION DE VERSIONES	
EQUIPO	Responsable de seguridad y Equipo de Soporte informático
OBJETIVO	Revisión de todos los sistemas de software de la compañía para verificar su estado y tener claro sobre la cantidad que se deberá trabajar a futuro.
DESCRIPCION	Para seguir un mismo patrón en toda la compañía se tendrán que tener una pauta establecida de las versiones de software con las que se deben trabajar, cada cuanto se deben revisar, cual es la versión mínima de software para poder trabajar etc. … Se deberá revisar mínimo una vez al año de que todo el software tenga instalada al menos la mínima versión de software admitida según la política.
BENEFICIO	Al tener las versiones actualizadas a las más recientes aparte de estar más protegidos, se disfrutarán de todas las nuevas herramientas que las actualizaciones puedan traer consigo.
RIESGO A MITIGAR	Software: Sistemas operativos, correo electrónico, aplicaciones, herramientas de desarrollo y herramientas de administración. Control: A.14.2
INICIO	5-06-2017
DURACION	1 mes
FIN	5-07-2017
PRESUPUESTO	1000 euros

Tabla 11: proyectos

c. Planificación:

Para hacerlo un poco más sencillo de visualizar a un golpe de vista en un diagrama resumiremos la planificación de los 3 proyectos.

Mayo				Junio						Julio		
10	15	20	30	5	10	15	20	25	30	5	10	15
	P_1											
			P_2									
				P_3								

Tabla 12: Planing

d. Resultado pos-mitigación:

Una vez aplicada la mitigación los valores quedaran como se puede ver en la siguiente tabla.

AMBITO	ACTIVO	FREC	IMP. POTENCIAL			RIESGO POTENCIAL		
			C	I	A	C	I	A
Hardware [HW]	Dispositivos para copias de seguridad	0.1-FB	10	4	8	1	0.4	0.8
	Cableado	1-FM	8	4.8	8	8	4.8	8
	Ordenadores	1-FM	8	4.8	10	8	4.8	10
	Servidor de archivos	1-FM	8	4.8	10	8	4.8	10
	Firewalls	1-FM	6	4.8	10	6	4.8	10
	Dispositivos de almacenamiento	0.1-FB	8	3	10	0.8	0.3	1
	Servidores de internet	0.1-FB	3.6	3	6	0.36	0.3	0.6
	Servidores de correo	0.1-FB	3.6	3	6	0.36	0.3	0.6
	Dispositivos móviles	0.1-FB	3.6	3	8	0.36	0.3	0.8
	Dispositivos de vigilancia	0.1-FB	6	5	10	0.6	0.5	1
	Dispositivos de salida (impresoras ...)	0.1-FB	6	3	4	0.6	0.3	0.4
	Servidores de impresión	0.1-FB	6	5	4	0.6	0.5	0.4
	Routers	0.1-FB	1	4	10	0.1	0.4	1
	Switches	0.1-FB	1	9	5	0.1	0.9	0.5
	Dispositivos de telefonía fija	0.1-FB	1.2	4	10	0.12	0.4	1
	Dispositivos virtuales	1-FM	3.6	4	10	3.6	4	10

	Aire acondicionado	0.1-FB	3	3	3	0.3	0.3	0.3
	UPS	1-FM	4	4	8	4	4	8
Software [SW]	Sistemas operativos	1-FM	6	8	10	6	8	10
	Correo electrónico	1-FM	10	6	8	10	6	8
	Aplicaciones	1-FM	6	8	8	6	8	8
	Herramientas de desarrollo	1-FM	6	6	6	6	6	6
	Herramientas administrativas	1-FM	6	6	8	6	6	8
Personal [P]	Persona con la autoridad para la toma de decisiones	1-FM	1.4	4	6.4	1.4	4	6.4
	Desarrolladores	0.01-FMB	0.8	1.6	3	0.008	0.016	0.03
	Personal de mantenimiento/operaciones	0.01-FMB	0.8	1.2	3	0.0008	0.012	0.03
	Usuarios	0.01-FMB	1	1.8	3	0.01	0.018	0.03
Infraestructura [INF]	Control de accesos	1-FM	0.1	3.2	7	0.1	3.2	7
	Comunicaciones	1-FM	1.2	4	8	1.2	4	8
	Sistema de refrigeración del edificio	1-FM	0.2	0.8	10	0.2	0.8	10
	CCTV (video vigilancia)	0.1-FB	0.4	1.6	4	0.04	0.16	0.4
	Servicios públicos (agua, electricidad, etc…)	0.1-FB	0.4	1.6	5	0.04	0.16	0.5
	Instalaciones	0.1-FB	0.6	2.4	10	0.06	0.24	1
	Habitaciones de comunicaciones	1-FM	0.6	2.4	10	0.6	2.4	10
Organización [ORG]	Autoridades	0.1-FB	0.4	1.2	4.8	0.04	0.12	0.48
	Políticas de empresa (locales, globales)	0.1-FB	0.4	1.6	10	0.04	0.16	1
	Procedimientos	0.1-FB	0.4	1.6	10	0.04	0.16	1
	Estándares	0.1-FB	0.4	1.2	6	0.04	0.12	0.6
	Estructura de la organización	0.1-FB	0.4	1.8	6	0.04	0.18	0.6
	Subcontratistas/Proveedores/Fabricantes	0.1-FB	0.4	1.8	10	0.04	0.18	1
Información [INF]	Datos de la compañía	1-FM	8	4.8	4.8	8	4.8	4.8
	Datos del cliente	1-FM	8	4.8	4.8	8	4.8	4.8

Tabla 13: Resultado pos-mitigación

➢ AUDITORIAS DE CUMPLIMIENTO:

1. INTRODUCCION:

Llegados a este punto conocemos los activos de la empresa y hemos evaluado las amenazas. Es momento de evaluar hasta qué punto la empresa cumple con las buenas prácticas en materia de seguridad.

2. METODOLOGIA:

Para el desarrollo de esta fase se usará el modelo de madurez de la capacidad (CMM) como metodologíaía para el análisis del grado de madurez en la implementaciónn del SGSI (Sistema de Gestión De Seguridad de la Información) en la implementación de la norma ISO 27001:2013, que agrupa un total de 114 controles. Esta estimación la realizaremos según la siguiente tabla, que se basa en el modelo de Madurez de la Capacidad que antes se ha comentado.

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
0 %	L0	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10 %	L1	Inicial/Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de veces en el esfuerzo personal. Los procesos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50 %	L2	Repetible pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90 %	L3	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95 %	L4	Gestionado y Medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100 %	L5	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Tabla 14: Modelo de capacidad para la madurez

3. EVALUACION DE LA MADUREZ:

El objetivo de esta fase del proyecto es evaluar la madurez de la seguridad en lo que respecta a los diferentes dominios de control y los 114 controles planeados por la ISO/IEC 27001:2013. Esta auditoría se lleva a cabo partiendo de que todos los proyectos del punto anterior se han ejecutado con éxito.

De forma resumida los dominios a analizar serán los siguientes:

- Política de seguridad.
- Organización de la seguridad de la información.
- Gestión de activos.
- Seguridad en los recursos humanos.
- Seguridad física y ambiental.
- Gestión de comunicaciones y operaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento de sistemas de información.
- Gestión de incidentes.
- Gestión de continuidad de negocio.
- Cumplimiento.

4	CONTEXTO DE LA ORGANIZACIÓN	Fase inicial	Fase final
4.1	COMPRENSION DE LA ORGANIZACIÓN Y DE SU CONTEXTO	95%	95%
4.2	COMPRENSION DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	95%	95%
4.3	DERMINACION DEL ALCANCE DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION	80%	80%
4.4	SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION	95 %	95 %
5	LIDERAZGO		
5.1	LIDERZGO Y COMPROMISO	90%	90%
5.2	POLITICA	80 %	80 %
5.3	ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACION	90%	90%
6	PLANIFICACION		

6.1	ACCIONES PARA TRATAR LOS RIESGOS Y OPORTUNIDADES			
6.1.1	CONSIDERACIONES GENERALES		95 %	95 %
6.1.2	APRECIACION DE RIESGOS DE SEGURIDADDE LA INFORMACION		95 %	95 %
6.1.3	TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACION		95 %	95 %
6.2	OBJETIVOS DE SEGURIDAD DE LA INFORMACION Y PLANIFICACION PARA SU CONSECUCION		95 %	95 %
7	SOPORTE			
7.1	RECURSOS		95 %	95 %
7.2	COMPETENCIA		95 %	95 %
7.3	CONCIENCIACION		95 %	95 %
7.4	COMUNICACION		95 %	95 %
7.5	INFORMACION DOCUMENTADA		95 %	95 %
7.5.1	CONSIDERACIONES GENERALES		95 %	95 %
7.5.2	CREACION Y ACTUALIZACION		95 %	95 %
7.5.3	CONTROL DE LA INFORMACION DOCUMENTADA		95 %	95 %
8	OPERACION			
8.1	PLANIFICACION Y CONTROL OPERACIONAL		95 %	95 %
8.2	APRECIACION DE LOS RIESGOS DE SEGURIDAD DE INFORMACION		95 %	95 %
8.3	TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE INFORMACION		95 %	95 %
9	EVALUACION DEL DESEMPEÑO			
9.1	SEGUIMIENTO, MEDICION, ANALISIS Y EVALUACION		95 %	95 %
9.2	AUDITORIA INTERNA		60 %	60 %
9.3	REVISION POR LA DIRECCION		95 %	95 %
10	MEJORA			
10.1	NO CONFORMIDAD Y ACCIONES CORRECTIVAS		50%	50%
10.2	MEJORA CONTINUA		90%	90%

5	POLITICAS DE SEGURIDAD		Fase inicial	Fase final
	5.1	**DIRECTRICES DE LA DIRECCION EN SEGURIDAD DE L A INFORMACION**		
	5.1.1	CONJUNTO DE POLITICAS PARA LA SEGURIDAD DE LA INFORMACION	80	95
	5.1.2	REVISION DE LAS POLITICAS PARA LA SEGURIDAD DE LA INFORMACION	80	95
6	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION**			
	6.2	**DISPOSITIVOS PARA MOVILIDAD Y TELETRABAJO**		
	6.2.1	POLITICA DE USO DE DISPOSITIVOS PARA MOVILIDAD	**80**	**95**
7	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**			
	7.1	**ANTES DE LA CONTRATACION**		
	7.1.1	**INVESTIGACION DE ANTECEDENTES**	70	70
8	**GESTION DE ACTIVOS**			
	8.1	**RESPONSABILIDAD SOBRE LOS ACTIVOS**		
	8.1.1	INVENTARIO DE ACTIVOS	70	70
	8.1.2	PROPIEDAD DE LOS ACTIVOS	70	70
	8.1.3	USO ACEPTABLE DE LOS ACTIVOS	70	70
	8.1.4	DEVOLUCION DE LOS ACTIVOS	70	70
	8.3	**MANEJO DE LOS SOPORTES DE ALMACENAMIENTO**		
	8.3.1	GESTION DE SOPORTES EXTRAIBLES	50	50
	8.3.2	ELIMINACION DE SOPORTES	50	50
	8.3.3	SOPORTES FISICOS EN TRANSITO	50	50
14	**ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION**			
	14.2	**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE**		
	14.2.3	REVISION TECNICA DE LAS APLICACIONES TRAS EFECTUAR CAMBIOS EN EL SISTEMA OPERATIVO	**80**	**95**
	14.2.4	RESTRICCIONES A LOS CAMBIOS EN LOS PAQUETES DE SOFTWARE	**80**	**95**
15	**RELACIONES CON SUMINISTRADORES**			
	15.1	**SEGURIDAD DE LA INFORMACION EN LAS RELACIONES CON SUMINISTRADORES**		
	15.1.1	POLITICA DE SEG. DE LA INFORMACION PARA SUMINISTRADORES	50%	50%
	15.1.2	TRATAMIENTO DEL RIESGO DENTRO DE ACUERDOS DE SUMINISTRADORES	50%	50%
	15.1.3	CADENA DE SUMINISTRO EN TECNOLOGIAS DE LA INF. Y CONMUNICACIONES	50%	50%
17	**ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DEL NEGOCIO**			
	17.1	**CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION**		
	17.1.1	PLANIFICACION DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION	**50 %**	**95 %**
	17.1.2	IMPLANTACION DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION	**50 %**	**95 %**
	17.1.3	VERIFICACION, REVISION Y EVALUACION DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION.	50 %	95 %
	17.1.1	PLANIFICACION DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION	50 %	95 %
	17.2	**REDUNDANCIAS**		
	17.2.1	DISPONIBILIDAD DE INSTALACIONES PARA EL PROCESAMIENTO DE LA INFORMACION	50 %	95 %

Tabla 15: Resumen de controles

4. PRESENTACION DE RESULTADOS:

A continuación, se muestra el resultado de las valoraciones para cada uno de los controles de la norma a modo resumen en una tabla para una mejor comprensión. Compararemos el estado inicial con el estado una vez aplicados los planes de trabajo de la fase anterior.

En la siguiente gráfica vemos un resumen de los controles y el nivel en el que se encuentran. Según el modelo de madurez que se ha utilizado(CMM) el 40% de los controles está en condiciones óptimas.

Por el contrario, existen controles con un nivel L3(90% o menor) o un nivel L2(50% o menor) sumando 7 controles a los cuales se les deberá prestar especial atención en próximas revisiones.

Controles y norma		
CMM	Antes	Después
L4(95%)	20	30
L3(90%)	16	11
L2(50%)	12	7

Tabla 16: total de controles antes y después

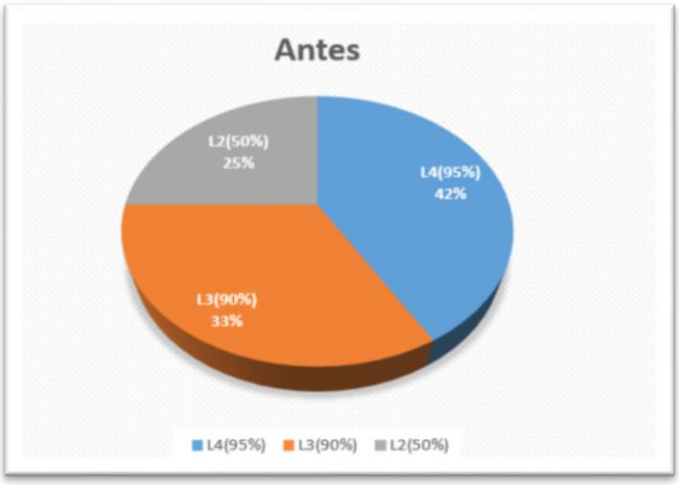

Figura 4: Resumen total controles a priori

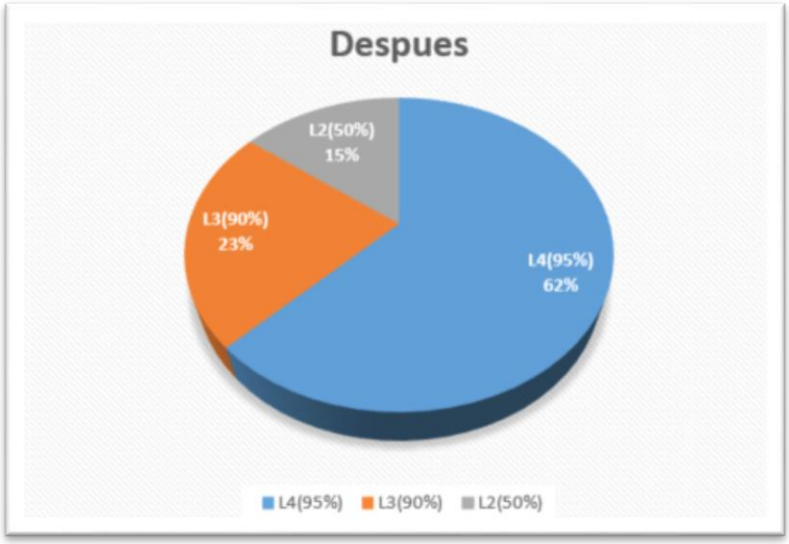

Figura 5 : Resumen total controles a posteriori

A continuación, podremos ver el resumen de las no conformidades obtenidas en la auditoría y acto seguido se podrá ver la auditoria en detalle.

La evaluación en esta auditoria se regirá según los siguientes niveles de inconformidad.

TIPO	DESCRIPCION
No conformidad mayor	Se incumple por completo un apartado del estándar.
No conformidad menor	Se incumple un punto del estándar o se incumple un procedimiento propio de la organización.
Observación	No se incumple nada, pero si no se hace un tratamiento adecuado, en el futuro se puede convertir en no conformidad menor.
Oportunidad de mejora	Es solo una recomendación, que nunca se convertirá ni en observación ni en no conformidad.

Tabla 17: Descripción de las no conformidades

Puntos de la norma & Controles	No conformidades			
	No conf. mayor	No conf. menor	Obsv.	Mejora
4 - CONTEXTO DE LA ORGANIZACIÓN				
4.3 - DERMINACION DEL ALCANCE DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION			**1**	
5 - LIDERAZGO				
5.2 - POLITICA			**1**	
9 – EVALUACION DEL DESEMPEÑO				
9.2 - AUDITORIA INTERNA		**1**		
10 - MEJORA				
10.1 – NO CONFORMIDAD Y ACCIONES CORRECTIVAS	**1**			
7 - SEGURIDAD LIGADA A LOS RECURSOS HUMANOS				
7.1.1 - INVESTIGACION DE ANTECEDENTES		1		
8 - GESTION DE ACTIVOS				
8.1.1 - INVENTARIO DE ACTIVOS		1		
8.1.2 - PROPIEDAD DE LOS ACTIVOS		1		
8.1.3 - USO ACEPTABLE DE LOS ACTIVOS		1		
8.1.4 - DEVOLUCION DE LOS ACTIVOS		1		
8.3.1 - GESTION DE SOPORTES EXTRAIBLES		1		
8.3.2 - ELIMINACION DE SOPORTES		1		
8.3.3 - SOPORTES FISICOS EN TRANSITO		1		
11 - SEGURIDAD FISICA Y AMBIENTAL				
11.1.1 - PERIMETRO DE SEGURIDAD FISICA		1		
11.1.2 - CONTROLES FISICOS DE ENTRADA		1		
11.1.3 - SEGURIDAD DE OFICINAS, DESPACHOS Y RECURSOS		1		
11.1.4 - PROTECCION CONTRA LAS AMENAZAS EXTERNAS Y AMBIENTALES		1		
15 - RELACIONES CON SUMINISTRADORES				
15.1.1 - POLITICA DE INFORMACION PARA SUMINISTRADORES		1		
15.1.2 - TRATAMIENTO DEL RIESGO DENTRO DE ACUERDOS DE SUMINISTRADORES		1		
15.1.3 - CADENA DE SUMINISTRO EN TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES		1		

Tabla 18: Tabla resumen no conformidades

Tipo de auditoria:	Interna
Normativa:	ISO 27001
Persona auditada:	Responsable de seguridad del centro
Auditor:	Auditor interno_1
Sede auditada:	Asturias, edificio II
Fecha:	1 de Mayo de 2017

Nº no conformidad	1
Area:	Contexto de la organización
Tipo de no conformidad	Observacion.
Control incumplido:	4.3 - Determinación del alcance del sistema de gestión de seguridad de la información.
Descripción:	No está del todo claro el alcance del sistema.
Acción correctiva:	Definir bien el alcance una vez que todos los sistemas estén instalados en el nuevo emplazamiento.
Fecha de revisión	1 de Junio de 2017
Nº no conformidad	2
Area:	Liderazgo
Tipo de no conformidad	Observacion.
Control incumplido:	5.2 - Política
Descripción:	Debido a cambios internos no está del todo clara la nueva política que se deberá de tener en cuenta.
Acción correctiva:	Revisar y actualizar en caso de ser necesario la nueva política.
Fecha de revisión	1 de Junio de 2017

Nº no conformidad	3
Area:	Evaluación del desempeño
Tipo de no conformidad	Menor
Control incumplido:	9.2 - Auditoria interna
Descripción:	No se realizan las auditorias con la periodicidad que se debería ni se envían los resultados al equipo global.

Acción correctiva:	Realizar un calendario de auditorías anual para seguir las fechas estipuladas, así como el seguimiento y el envío del informe al equipo global.
Fecha de revisión	1 de Junio de 2017
Nº no conformidad	4
Area:	Mejora
Tipo de no conformidad	Mayor
Control incumplido:	10.1 – No conformidad y acciones correctivas
Descripción:	No se realiza el seguimiento apropiado de las auditrias internas ni se hace un seguimiento correcto para solucionar los problemas encontrados en ellas.
Acción correctiva:	Hacer seguimiento y dar solución a todos los puntos pendientes de revisar hasta la fecha actual.
Fecha de revisión	1 de Junio de 2017

Nº no conformidad	5
Area:	Seguridad ligada a los recursos humanos
Tipo de no conformidad	Menor
Control incumplido:	7.1.1 - Investigación de antecedentes
Descripción:	Ante un nueva alta en la empresa se deberán de realizar una serie de comprobaciones en el pasado laboral del individuo. Comprobando la veracidad de su experiencia, reseñas y estudios.
Acción correctiva:	Se deberá de realizar una investigación de cada uno de los candidatos sin excepción, comprobando referencias, experiencia así como formación.
Fecha de revisión	1 de Junio de 2017
Nº no conformidad	6
Area:	Gestion de activos
Tipo de no conformidad	Menor
Control incumplido:	8.1.1 - Inventarios de activos 8.1.2 - Propiedad de los activos 8.1.3 - Uso aceptable de los activos 8.1.4 - Devolución de los activos 8.3.1 - Gestión de soportes extraíbles 8.3.2 - Eliminación de soportes 8.3.3 - Soportes físicos en tránsito

Descripción:	No existe inventario de activos actualizado. No está clara la propiedad de los activos. No se está verificando si se hace un uso aceptable de los activos. No existe un procedimiento de entrega de materiales ante la baja de los empleados. Se deben tener controlados todos los sistemas de almacenamiento portátiles como discos duros, lápices de almacenamiento. Cuando se elimina información ya bien sea física o electrónica se debe asegurar que sea de forma segura y que nadie podrá acceder a la información. Cuando los sistemas que contienen información salen fuera de la empresa se deberán de seguir unas pautas concretas para que sea seguro su transporte.
Acción correctiva:	Inventariar todos los dispositivos y mantenterlo actualizado.
Fecha de revisión	1 de Junio de 2017

Nº no conformidad	7
Area:	Seguridad fisica y medioambiental
Tipo de no conformidad	Menor
Control incumplido:	11.1.1 – Perímetro de seguridad física 11.1.2 – Controles físico de entrada 11.1.3 – Seguridad de oficinas, despachos y recursos. 11.1.4 – Protección contra las amenazas externas y ambientales.
Descripción:	No existe un perímetro de seguridad totalmente finalizado. Aún no están instalados todos los controles fisico de seguridad, están en proceso de los detectores de intrusión y todo el sistema de accesos. Aún no están instalados los controles de seguridad en las salas y despachos. El sistema anti-intrusión que ayuda a impedir o notificar cuando se produce alguna amenaza, está en proceso de instalación.
Acción correctiva:	Revisar en unos 15 dias para asegurarse de que el sistema anti-intrusion y el sistema de control de accesos está totalmente instalado y en funcionamiento.
Fecha de revisión	22 de Mayo de 2017

Nº no conformidad	8
Area:	Relaciones con suministradores

Tipo de no conformidad	Menor
Control incumplido:	15.1.1 – Política de información para suministradores. 15.1.2 – Tratamiento del riesgo dentro de acuerdos de suministradores. 15.1.3 – Cadena de suministro en tecnologías de la información y comunicaciones.
Descripción:	No existe una política adecuada de cómo debe ser el tratamiento con respecto a los proveedores externos.
Acción correctiva:	Crear una política adecuada de cómo debe ser el tratamiento con respecto a los proveedores externos.
Fecha de revisión	1 de Junio de 2017

Después de llevar a cabo todas las fases de este proyecto se ha producido una mejora en el sistema, no obstante, y tal como se puede ver en la tabla resumen de no conformidades aún quedan varias de ellas que impiden que el sistema esté en el nivel L3, según el CMM.

Son no conformidades menores en su mayoría y observaciones, y solo existe una no conformidad mayor, su próxima revisión será el 1 de Junio de 2017 por lo que para esa fecha con gran probabilidad varias de ellas estarán subsanadas.

➢ **PRESENTACION DE RESULTADOS Y ENTREGA DE INFORMES.**

Esta información tal y como se indica debe ir en una presentación de power point, así como la presentación final del trabajo.

ANEXOS:

A - POLITICA DE SEGURIDAD

Autor	XXXXX XXXXX
Creación del documento	dd mm aaaa
Propietario del documento	XXXXXXXXX
Referencias	xxxxxxxxxx
Versión	1.1
Estado	Revisada y aprobada.
Última versión	XXXXXXXXX

Tabla de cambios:

Version#	Fecha	Autor	Comentario
1	XXXXX	XXXXX	Version inicial
1.1	XXXXX	XXXXX	Revisada y aprobada

La **COMPAÑIA** considera que la información, en cualquier forma, es un activo de la empresa y requiere controles adecuados para proteger estos activos de todas las amenazas, ya sean internas o externas, deliberadas o accidentales.

La información es vital para el funcionamiento eficiente y efectivo de la corporación. Dicha información sólo debe utilizarse para los fines previstos, es decir, para la realización de las operaciones comerciales de la **COMPAÑIA**. La política de la **COMPAÑIA** es proporcionar acceso a la información únicamente en base a una base probada de "necesidad de información empresarial" y denegar el acceso a todos los demás.

Es también la política de la **COMPAÑIA** garantizar la continuidad del negocio y minimizar el impacto de los incidentes de seguridad, asegurando que mantenemos los tres aspectos de la Seguridad de la Información:

• **CONFIDENCIALIDAD** - proteger información valiosa y sensible de la divulgación no autorizada.

• **INTEGRIDAD** - salvaguardar la exactitud e integridad de la información.

• **DISPONIBILIDAD** - asegurar que la información y los servicios vitales estén disponibles para los usuarios.

Para garantizar estos aspectos de la información, la **COMPAÑIA** refuerza:

• **RESPONSABILIDAD** - Las acciones realizadas por un individuo a la información pueden ser rastreadas únicamente para ese individuo.

• **MENOS PRIVILEGIOS** - Cada usuario tendrá acceso a los activos de información basados en los principios de "necesidad de saber" y "necesidad de hacer" según lo requiera su rol en el trabajo.

Nº no conformidad	3
Area:	Seguridad física y medioambiental
Tipo de no conformidad	Menor
Control incumplido:	11.1.1 - Perímetro de seguridad física 11.1.2 - Controles físicos de entrada 11.1.3 - Seguridad de oficinas, despachos y recursos 11.1.4 - Protección contra las amenazas externas y ambientales
Descripción:	No existe un perímetro de seguridad totalmente finalizado. Aun no están instalados todas los controles físicos de seguridad, están en proceso los detectores de intrusión y todo el sistema de control de accesos. Aun no están instalados los controles de seguridad en las salas y despachos. El sistema anti-intrusion que ayuda a impedir o notifica cuando se produce alguna amenaza está en proceso de instalación.
Acción correctiva:	Revisar en unos 15 días para asegurarse de que el sistema anti-intrusión y el sistema de control de accesos está totalmente instalado y en funcionamiento.
Fecha de revisión	22 de Mayo de 2017

Nº no conformidad	4
Area:	Relaciones con suministradores
Tipo de no conformidad	Menor
Control incumplido:	15.1.1 - Política de información para suministradores 15.1.2 - Tratamiento del riesgo dentro de acuerdos de suministradores. 15.1.3 - Cadena de suministro en tecnologías de la información y comunicaciones.
Descripción:	No existe una política adecuada de como debe ser el tratamiento con respecto a los proveedores externos.
Acción correctiva:	Crear una política que especifique como debe ser la relación entre la empresa y los proveedores en cuanto a seguridad de la información se refiere.
Fecha de revisión	1 de Junio de 2017

• **SEGREGACIÓN DE LOS DEBERES** - Los deberes y el área de responsabilidad serán segregados para reducir las oportunidades de modificación no autorizada o no intencional o el uso indebido de la organización

• **ESCALABILIDAD**- Se mantendrá la arquitectura de seguridad, de manera que se puedan acomodar las diferentes necesidades de seguridad de la organización.

Esta política complementa las políticas de seguridad de LA **COMPAÑIA**, diseñadas para garantizar que LA **COMPAÑIA** opera en un entorno seguro; Que protege los intereses

de los empleados, la empresa y los clientes de la empresa. Cuando los requisitos legales, regulatorios y contractuales de España son más estrictos que las políticas de seguridad corporativa o global, las políticas de seguridad de LA **COMPAÑIA** (y procedimientos) prevalecen.

1 Alcance:

La política de seguridad de la información de la **COMPAÑIA** se aplicará a:

• Todos sus funcionarios y empleados de la **COMPAÑIA** ubicados en, o trabajando desde sitios de la **COMPAÑIA**.

• Todos los empleados y agentes de otras Divisiones la **COMPAÑIA** que apoyan a la **COMPAÑIA**

• Todos los socios, contratistas, proveedores, sus empleados y agentes que apoyen directa o indirectamente a la **COMPAÑÍA.**

2 Objetivo:

• Asegurar que se proporcione una adecuada protección contra las amenazas a la información de la **COMPAÑIA**, garantizando así la Confidencialidad, Integridad y Disponibilidad de la información adecuada a las necesidades empresariales.

• Asegurar que los activos de la **COMPAÑIA** estén protegidos y permanezcan disponibles.

• Asegurar que la **COMPAÑIA** implemente y mantenga el estándar mínimo de seguridad definido en las políticas de seguridad global de la **COMPAÑIA** o definido en cualquier Normativa, certificado o política aplicable.

• Asegurar que la información de la **COMPAÑIA**, compartida con otras partes, esté protegida contra la divulgación no autorizada y se gestione de acuerdo con esta política.

• Asegurar que la **COMPAÑIA** implemente los requisitos de ISO 27002 - Un Código de Prácticas para la Gestión de la Seguridad de la Información donde sea posible.

• Mantener el ISMS ISO27001 y la certificación donde se especifique.

• Velar por que todos los funcionarios, empleados y contratistas de España conozcan y cumplan los requisitos legales y reglamentarios aplicables en materia de TI; Concretamente en la legislación española de la **COMPAÑÍA.**

• Crear y mantener la conciencia de la gestión y del personal de la **COMPAÑIA** sobre la seguridad de la información, garantizando así que todos los empleados entiendan su importancia para la **COMPAÑIA** y sus propias responsabilidades individuales en materia de seguridad.

• Asegurar que sólo se utilice equipo autorizado para procesar la información comercial de la **COMPAÑÍA**.

• Asegurar que las personas que desempeñan funciones de seguridad identificadas reciban una formación especializada en consonancia con sus responsabilidades en materia de seguridad.

• Asegurar que todas las infracciones de seguridad de la información, reales o sospechadas, sean reportadas e investigadas por el Departamento de Seguridad de España.

3 Responsabilidades:

La seguridad es un problema para todos. Cada empleado debe adherirse a esta política (y apoyar políticas globales), directrices y procedimientos. Los empleados que no cumplan con estas directivas serán responsables de acciones disciplinarias.

Cada cuenta es en última instancia responsable de asegurar que los requisitos de seguridad de la información del cliente se cumplan y se implementan de acuerdo con las obligaciones contractuales y la legislación. También son responsables de la Continuidad de Negocio de su cuenta y del Análisis de Impacto Empresarial de sus necesidades. Cuando la cuenta es interna de la **COMPAÑÍA**, esta responsabilidad recae en el Departamento de Seguridad.

Cada área funcional es responsable de:

• Asegurarse de que cumplen con la política de gestión de información y registro de MPS 902.

• Toda la información debe ser propiedad, identificada, inventariada y debidamente clasificada de acuerdo con su valor y las normas y directrices de la **COMPAÑÍA.**

Cuando cualquier posición antes mencionada no se asigna cae en un comité formado por el Director, el personal de Gestión de la Entrega y Seguridad.

B – PROCEDIMIENTO DE AUDITORIA INTERNA

Versión	Fecha	Autor	Descripción
0.1	XXXXXXX	XXXXXXX	Borrador inicial
1.0	XXXXXXX	XXXXXXX	Actualizado y modificado para seguir la misma línea del certificado global y el SGSI.
1.1	XXXXXXX	XXXXXXX	Propiedad modificada del documento y aprobadores para reflejar los cambios en el Manual SGSI
1.2	XXXXXXX	XXXXXXX	Revision anual
1.3	XXXXXXX	XXXXXXX	Actualización.
1.4	XXXXXXX	XXXXXXX	Revision

y requisitos externos especificados para cumplir con las metas y objetivos de la COMPAÑIA en relación con su postura de gestión de la seguridad de la información.

1.2 Asegurar que las deficiencias y mejoras al SGSI se identifiquen claramente y cuando sea necesario: de acuerdo con las acciones correctivas requeridas, implementadas y consideradas adecuadas para lograr los objetivos del SGSI y se realiza como parte de un proceso de auditoría interna independiente para asegurar segregación razonable de los derechos.

2.0 Alcance

2.1 Este procedimiento es específico para todas las ubicaciones definidas por el alcance de dicho SGSI e incluye: planificación, ejecución, notificación y requisitos de seguimiento como parte de la auditoría interna del SGSI y se aplica a todos los departamentos y servicios definidos como dentro del alcance del SGSI.

3.0 Responsabilidades de Auditoría Interna

3.1 Representante de Gestión de la Seguridad de la Información (ISMR)

- Nombra al Auditor Principal y al Equipo de Auditoría (El Equipo de Auditoría). El Auditor Principal también puede ser el ISMR.
- El Equipo de Auditoría revisa las acciones Correctivas y Preventivas para dicho lugar y las auditorías de seguimiento realizadas sobre la base del informe de auditoría interna presentado.

- Mantiene la confidencialidad de los resultados de la auditoría.

3.2 Auditor principal

- Prepara un Plan de Auditoría / Notificación como base para la planificación de la auditoría y para la difusión de información sobre la auditoría.
- Preside las actividades de auditoría interna.
- Coordina el cronograma de auditoría con los jefes de departamento / sección interesados.
- Planifica la auditoría, prepara los documentos de trabajo e informa al equipo de auditoría.
- Consolidar todos los hallazgos y observaciones de auditoría y preparar el informe de auditoría interna.
- Reporta inmediatamente las no conformidades críticas a la parte auditada.
- Informar a la parte auditada, los resultados de la auditoría de forma clara y sin demora
- Realiza la reunión de apertura y cierre.

3.3 Equipo de auditoría

- Apoya las actividades del Auditor Líder.
- Realiza la auditoría utilizando la lista de comprobación de auditoría consolidada.
- Reporta las no conformidades y recomienda sugerencias para mejorar.
- Mantiene la confidencialidad de los hallazgos de la auditoría.
- Actuar de manera ética en todo momento.

3.4 Parte auditada

- Recibe el informe de auditoría y determina, así como inicia el seguimiento requerido de la (s) acción (es) correctiva (s).

4.0 Procedimiento de auditoría

4.1 General

4.1.1 Se debe mantener un programa de auditoría que refleje todas las auditorías programadas y planeadas para el año calendario de auditoría. Esto incluirá un cronograma de auditorías internas, auditorías realizadas a proveedores, auditoría a realizar por clientes y auditorías de terceros, cuando corresponda.

4.1.2 Cada lugar sujeto al SGSI de la COMPAÑIA estará sujeto a una auditoría interna anual. Pueden realizarse auditorías adicionales si un lugar en particular tiene un gran número de conclusiones en su contra.

4.1.3 Los auditores deben ser independientes de la ubicación en la que están obligados a realizar la auditoría, ya que no tienen obligación de rendir cuentas al centro sujeto a la auditoría.

4.1.4 Como se menciona en la Sección 3.1, todos los miembros del Equipo de Auditoría Interna serán nombrados por el ISMR.

4.1.5 El Auditor Principal supervisará la actividad del Equipo de Auditoría.

4.1.6 Se enviará un Memo de Notificación de Auditoría a la ubicación / departamento / sección para ser auditado por lo menos tres (5) días hábiles antes de la auditoría.

4.2 Planificación y preparación de la auditoría

4.2.1 El auditor principal elaborará un documento anual del programa de auditoría y será aprobado por el responsable del programa del SGSI y estará sujeto a revisión de acuerdo con los cambios en el calendario.

4.2.2 A partir de este programa de auditoría, el Auditor Líder preparará los respectivos planes de auditoría.

4.2.3 El Auditor de Cuentas / Notificación deberá ser preparado por el Auditor Líder, revisado y aprobado por el ISMR. Se comunicará a los auditores ya la parte auditada. Se diseñará para ser flexible con el fin de permitir cambios basados en la información recogida durante la auditoría. El plan incluirá:

- Objetivo y alcance de la auditoría
- Departamento / Sección y responsables.
- Miembros del equipo de auditoría. El número de auditores depende del tamaño del área de auditoría.
- Tipo de sistema de gestión a auditar
- Fecha, lugar, hora de la auditoría y fecha de distribución del informe de auditoría

4.3 Reunión previa a la auditoría

4.3.1 La reunión previa a la auditoría entre el ISMR, el auditor principal y los auditores se llevará a cabo a más tardar un día antes de la auditoría propiamente dicha. Los objetivos son los siguientes:

- Asegurar la disponibilidad de todos los recursos necesarios y otra logística que pueda requerir el auditor.
- El alcance de la auditoría se verifica en el Plan de Auditoría

4.4 Reunión de apertura

4.4.1 La reunión de apertura, cuando lo considere apropiado el ISMR y el auditor principal, se celebrará el día de la auditoría, pero antes de la auditoría propiamente dicha. Durante la reunión de apertura se discutirá lo siguiente:

- El propósito y alcance de la auditoría.
- Confirmación del plan de auditoría
- Es necesario aclarar otros asuntos antes de que se realice la auditoría

4.5 Ejecución de auditoría

4.5.1 Los auditores realizarán la auditoría interna utilizando varias listas de verificación que se describen a continuación:

- Lista de Verificación de Auditoría Interna / Formulario de Observación- contiene elementos específicos que son específicos de la unidad organizacional a ser auditada. Los auditores asignados son responsables de generar preguntas usando este formulario.
- La Lista de Verificación de Requisitos del Sistema contiene elementos relacionados con los requisitos de ISO 27001: 2013
- Lista de verificación de los requisitos de control - contienen elementos relacionados con los controles que se encuentran en el Apéndice A de la Norma ISO 27001: 2013.
- Los resultados de la auditoría se recogen a través de entrevistas, examen de documentos y observación de actividades y condiciones en las áreas de preocupación y se escribirán en las listas de verificación mencionadas anteriormente.
- Evidencias que sugieren no conformidades deben ser anotadas sí parecen significativas, aunque no estén cubiertas por la lista de verificación. Otras indicaciones y/u observaciones objetivas que puedan reflejarse positivamente o negativamente en el sistema de gestión de la seguridad de la información también se enumerarán en el espacio previsto en las listas de verificación antes mencionadas.

[…]

C – REVISION POR LA DIRECCION - ACTAS DE REUNION

ISO 27001:2013 REVISION CON LA DIRECCION

Nombre	Cargo	Presente
XXXXXXXXX	DIRECTOR DEL CENTRO	✔
XXXXXXXXX	RESPONSABLE DE SEGURIDAD	✔

FECHA, HORA, LUGAR:

Fecha	Hora:	Lugar:
dd/mm/aaaa	Xx:xx	Calle, numero, Provincia, Pais

OBJETIVO DE LA REUNION:

Management review of the ISMS system to ensure suitability, adequacy and effectiveness. The review is to include the assessment of opportunities for improvement and any potential changes in the normative, including security policy and objectives, and their alignment with business objectives and strategy.

AGENDA:

Revisar acciones de las notas de reunión

▪ Revisar y aprobar las notas de la reunión anterior.
▪ Revisar el estado de las acciones pendientes.
▪ Registrar el estado de las acciones en curso.
▪ Cerrar las acciones completas.
Resultados de la auditoria interna – No conformidades
▪ Revisar el estado.
Metricas
▪ Revisar las métricas
▪ Revisar los resultados de los incidentes así como de la solución y/o el seguimiento.
Gestión de riesgos
▪ Revisar la gestion de riesgos y los riesgos vigentes – Cuando sea aplicable (dos veces al año)
Revisar calendario de eventos
SGSI revisión
▪ Revisar/confirmar los puntos del SGSI
✓ *Alcance*
✓ *Notas de reuniones locales* ➔*Obligatorio, punto*
✓ *Politicas locales*
✓ *Politicas globales*
✓ *Roles y responsabilidades*
✓ *Gestion de riesgos.*
✓ *Declaracion de aplicabilidad*
✓ *Gabinete de crisis local.*
✓ *Metricas* ➔*Obligatorio, punto 3*
✓ *Formacion de seguridad inicial*
✓ *Programa de auditoria interna*
✓ *Acciones preventivas y correctivas*
▪ Revisión de la ejecución y la mejora continua del SGSI - Obligatorio
▪ Bajo demanda ….
Recomendaciones para la mejora
Cierre de reunion
Confirmar acciones y autores.

	Confirmar tiempos para las acciones
	Confirmar fecha y hora de la siguiente reunión.

D – ROLES Y RESPONSABILIDADES

SGSI Roles y responsabilidades (procedimiento interno)

Autor

Fecha del documento dd mm aaaa

Responsable del documento	xxxxxxxxxxxx
Version	1.1
Estado	Version inicial
Repositorio	xxxxxxxxxxxxxxxxxxxxx
Clasificación del documento	xxxxxxxxx

Version#	Fecha	Autor	Comentario
1	XXXXX	XXXXX	Version inicial
1.1	XXXXX	XXXXX	Revisada y aprobada

1**. Propósito**

Asegurar que se estén aplicando todas las funciones de seguridad requeridas por el SGSI y que sus competencias principales estén correctamente identificadas.

2**. Alcance**

Este procedimiento es específico para el ISMS del centro.

Asegurar que el SGSI del Centro funcione de acuerdo con la definición de Roles de Seguridad especificada en todos los Documentos de Seguridad Global del SGSI.

3. Roles

3.1 Operaciones de Seguridad y Roles de Gobierno:

- **Gerente del Centro(dirección):** es responsable de la Seguridad en el sitio incluyendo la seguridad física, de la información y la continuidad del negocio del centro. Responsable de las revisiones de la gerencia para el ISMS.
- **Director global de ciberseguridad:** como Líder Global del Programa de Seguridad del SGSI, es el Aprobador del SGSI y responsable de la revisión y aprobación de los documentos, registros y gobierno del SGSI.

Competencias clave: Fuertes habilidades de comunicación para interactuar con representantes de alto nivel del cliente

- **Gerente de Auditoría y Servicios de Seguridad de la Información:** es el propietario global de SGSI y responsable de todas sus entradas, procesos, documentación y mantenimiento a nivel de Europa. El Propietario global del SGSI nombrará a los delegados según sea necesario para desempeñar funciones de administración de documentación y para dirigir actividades de certificación o mantenimiento, incluyendo nuevos proyectos de certificación.

  Competencias clave: Fuertes habilidades de comunicación necesarias para interactuar con representantes de alto nivel del cliente

- **Oficial de Protección de Datos:** es responsable de asegurar que la ley aplicable a la privacidad de los datos cumpla con las cuentas y contratos internos. Aprobación de las normas y directrices de seguridad de la compañía antes de su emisión.

  Competencias clave: Fuertes habilidades de comunicación para comunicarse con proveedores, personal, personal de la compañía y para documentar información. Conocimiento fuerte de la legislación aplicable de privacidad de datos.

- **Responsable de seguridad de centro:** es responsable de:

  - Asegurar que la Política, Normas y Directrices de Seguridad de la Información de que la empresa en España cumpla con las responsabilidades legales y regulatorias españolas.
  - Tomar decisiones de riesgo de seguridad de la información para riesgos de seguridad mayores recomendando acciones para la alta aprobación de la gerencia.
  - Presentación periódica del informe sobre el estado de seguridad de la información de la compañía a la alta dirección.
  - Proporcionar un punto focal para las cuestiones y asesoramiento de la compañía sobre Seguridad de la Información.
  - Proporcionar Inducción de Seguridad, y otros capacitadores y conciencia cuando son necesarios

Competencias clave: Capacidad para mantener confidencial el material confidencial y confidencial. Buena capacidad de comunicación.

- **Guardia de seguridad:** proporciona un ambiente seguro para el personal y los visitantes patrullando y proporcionando acceso a las instalaciones, etc., de acuerdo con las políticas y procedimientos de la organización.

  Competencias clave: capacidad para tratar con los demás de una manera cortés y cortés. Se puede requerir trabajo de turno.

3.2 Funciones de emergencia

- **Gerente de Crisis:**
    - El Gerente de Crisis será responsable de liderar y activar el Equipo de Manejo de Crisis (SAMT) cuando sea necesario.
    - Iniciando el contacto con el Centro de Gestión de Crisis, escalar la naturaleza del incidente dentro de los niveles ejecutivos de la empresa y el cliente.
    - Garantizar la organización completa para hacer frente a la crisis.
    - Tendrá plena autorización de todas las decisiones de invocación y la implementación o instigación de los procesos de mitigación de riesgos durante el ciclo de vida del incidente
    - Además, el Gerente de Crisis y el Gerente de Seguridad de Instalaciones también serán responsables de asegurar que los planes de continuidad de negocios se mantengan y se ejerzan regularmente de acuerdo con el programa de pruebas acordado.

  Competencias clave: Buenas habilidades interpersonales para interactuar con clientes y miembros del equipo. Capacidad para trabajar bajo presión. Capacidad para responder rápidamente a eventos imprevistos.

- **Coordinador de Seguridad:** será responsable de lo siguiente:
    - Evaluar los métodos alternativos de trabajo y las estrategias de recuperación de negocios para asegurar que se mantengan las políticas y medidas de seguridad requeridas.
    - Cuando los métodos o procedimientos de trabajo de continuidad requieran medidas de seguridad alternativas, verifique con la agencia los protocolos y procedimientos alternativos y la posible relajación de la política cuando sea necesario y / o apropiado.
    - Asesorar al Equipo de Gestión de Crisis de cualquier riesgo potencial y / o amenaza
    - Coordinar e implementar todos los procedimientos revisados, cuando se requieran medidas de seguridad alternativas
    - Administrar y monitorear el cumplimiento de los riesgos de seguridad durante dichos períodos de métodos operativos alternativos.

  Competencias clave: Buenas habilidades interpersonales para interactuar con clientes y miembros del equipo. Capacidad para trabajar bajo presión.

- **Coordinadora de Continuidad de Negocios:** el coordinador de Continuidad de Negocio proporcionará apoyo al Gerente de Crisis en lo siguiente:
    - Orientación sobre la implementación de planes de continuidad de negocio.
    - Registrar todos los problemas y monitorear el proceso de recuperación.
    - Coordinar las llamadas de emergencias.
    - Nombrar un asistente para ayudar con la documentación del proceso de recuperación.
    - Facilitar la coordinación de recursos y proveedores de servicios.

    Competencias clave: Buenas habilidades interpersonales para interactuar con clientes y miembros del equipo. Capacidad para trabajar bajo presión.

3.3 Funciones de garantía de seguridad:

- Auditor Principal:
    - Prepara un Plan de Auditoría / Notificación como base para planificar la auditoría y para difundir información sobre la auditoría.
    - Preside las actividades de auditoría interna.
    - Coordina el programa de auditoría con los jefes de departamento / sección interesados.
    - Planifica la auditoría, prepara los documentos de trabajo e informa al equipo de auditoría.
    - Consolidar todos los hallazgos y observaciones de auditoría y preparar el informe de auditoría interna.
    - Reporta inmediatamente las no conformidades críticas a la parte auditada.
    - Informar a la parte auditada, los resultados de la auditoría de forma clara y sin demora
    - Realiza la reunión de apertura y cierre.

- **Representante de Gestión de Seguridad de la Información:**
    - Designa al auditor principal y al equipo de auditoría (el equipo de auditoría). El auditor principal también puede ser el ISMR.

- El Equipo de Auditoría revisa las acciones Correctivas y Preventivas para dicho lugar y las auditorías de seguimiento realizadas sobre la base del informe de auditoría interna presentado.
- Mantiene la confidencialidad de los resultados de la auditoría.

Competencias clave: habilidades en el liderazgo de auditoría para facilitar la realización eficiente y efectiva de la auditoría. Deberían tener conocimientos sobre la terminología de seguridad de la información.

BIBLIOGRAFIA

1. https://advisera.com/27001academy/es/que-es-iso-27001/
2. http://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001/
3. http://www.pmg-ssi.com/2015/05/iso-27001-analizar-y-gestionar-riesgos-sgsi/
4. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html