IMPLEMENTACIÓN ISO 27001 – EMPRESA FICTICIA

SARA CUERVO ALVAREZ

PRESENTACION

Sara Cuervo Alvarez

28 años

Ingeniera técnica de Telecomunicaciones

Trabajo actual: Empresa del sector TIC – departamento de ciberseguridad

Introducción

- 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.
- Este trabajo se dividirá en varias partes las cuales serán:
  - 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.

Introducción:

- La compañía sobre la que vamos a trabajar se sitúa en Asturias y tiene alrededor de unos 1000 empleados.
- Es una compañía estadounidense que da soporte a multiples clientes tanto nacionales como internacionales.
- Es una compañía que ya ha tenido sus primeros contactos con la ISO 27001 puesto que parte de ella ya tiene una certificación.
- Los principales servicios que esta compañía proporciona son: servicios de aplicaciones, servicios en la nube, consultoría, seguridad, banca, seguros, sector público global.
- El alcance sobre el que trabajaremos serán:
  - 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.
  - Toda la información generada durante la vida del negocio para los proyectos.
  - La información de empleados, clientes, proveedores de servicios, etc

- Conociendo la iso 27001:
  - Como todos bien sabemos ISO es una norma internacional emitida por la organización internacional de normalización y describe como gestionar la seguridad de la información en una empresa. La revisión mas reciente de la norma fue la de 2013.
  - 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 y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan.
  - 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.
- 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

- 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.

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.
- ANALISIS 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 de los controles obligatorios de la norma superan en su mayoría el 80% exceptuando algunos como:
  - El punto número 9 – control de accesos.
  - El punto numero 10 - Mejora
- El estado de los controles según la ISO 27002 también superan en su mayoría el 80 % exceptuando algunos como:

Punto 8 – Gestión de activos – 8.1 responsabilidad sobre los activos.

Punto 8 – Gestión de activos – 8.3 manejo de los soportes de almacenamiento.

Punto 11 – Seguridad física y ambiental – 11.1 áreas seguras.

Punto 15 – Relaciones con suministradores – 15.1 Seguridad de la información en las relaciones con los suministradores.

Punto 17 – Aspectos de seguridad de la información en la gestión de la continuidad de negocio – 17.1

Punto 17 – Aspectos de seguridad de la información en la gestión de la continuidad de negocio – 17.2 Redundancias

- Pasamos al punto del sistema de gestión documental:
  - Aquí se describirán los principales documentos para la ISO 27001.
    - Política de seguridad de la información:
      - Este punto es muy importante puesto que en el se describe la política de la información de la organización, uno de los documentos básicos. Esta dentro del apartado anexos de la memoria.
    - Procedimiento de auditorias internas:
      - Este documento describe el Procedimiento de Auditoría Interna para el SGSI. El principal objetivo y el alcance de este procedimiento de auditoria interna es:
        - El de 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.
        - Asegurar que las deficiencias y mejoras al SGSI se identifiquen claramente.
    - Métricas o gestión de indicadores:
      - Las métricas o los indicadores es una manera de medir como de eficientes son los controles implementados.
    - Procedimiento de revisión con la dirección.
      - 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.
    - Roles y responsabilidades:
      - La alta dirección de una organización debe asignar responsabilidades y autoridades para cada uno de los roles relativos a la seguridad de la información y esto debe quedar documentado en este documento.
    - Declaración de aplicabilidad:
      - 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.
    - Metodología de análisis de riesgos:

- 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.
  - Se definen también las fases que se llevaran a cabo en el análisis de riesgos.

ANALISIS DE RIESGOS

- Las fases que se llevaran a cabo en este punto serán:
  - Identificación-valoración de activos:
    - Se realizará una identificación, valoración de los activos, que serán los elementos a proteger.
    - Se ha realizado una tabla con todos los activos y su valoración, como se podrá ver en una imagen en la siguiente diapositiva.
  - Identificación de amenazas:
    - Identificar y valorar las amenazas a las que se encuentran expuestos estos activos.
    - Se ha realizado una tabla bastante extensa con todas las valoraciones teniendo en cuenta las siguientes amenazas: desastres naturales, de origen industrial, errores o fallos no intencionados y ataques intencionados. En la siguiente diapositiva se podrá ver una captura.
  - Calculo de 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.
    - Se adjunta imagen de la tabla con los valores obtenidos.
  - 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.
    - Se adjunta imagen de la tabla con los valores obtenidos.
  - 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.

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

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%

AMBITO	ACTIVO	CRITICIDAD			%IMPACTO			IMP. POTENCIAL		
		C	I	A	C	I	A	C	I	A
	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

AMBITO	ACTIVO	FREC	IMP. POTENCIAL			RIESGO POTENCIAL		
			C	I	A	C	I	A
	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

PROPUESTA DE PROYECTO

- 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.
- 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.
- Se puede ver el detalle de los proyectos en las capturas de la siguiente diapositiva.
- Todos los proyectos han tenido una planificación en el tiempo para su ejecución y una vez aplicados se observa el resultado obtenido para la valoración de los activos. Se puede ver una captura de pantalla en la siguiente diapositiva.

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

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

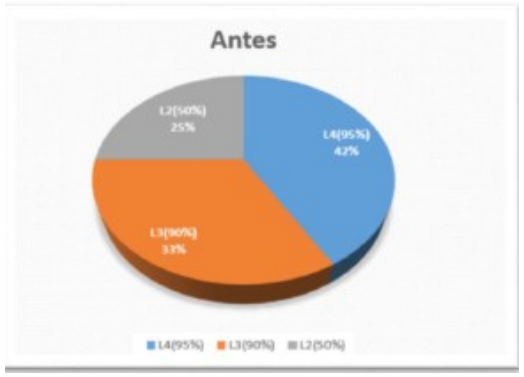
AUDITORIA DE CUMPLIMIENTO

- Llegamos al ultimo punto del proyecto.
- Ya 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.
- Para el desarrollo de esta fase se usará el modelo de madurez de la capacidad (CMM) como metodología para el análisis del grado de madurez en la implementación del SGSI.
- 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. Se realizará la comparación de la fase uncial con la fase final como se podrá ver en la captura de la siguiente diapositiva.

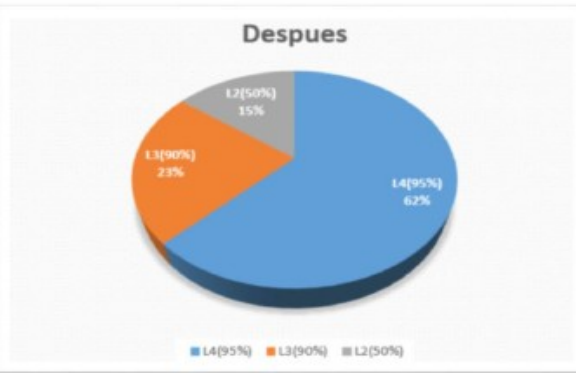
EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
0 %	L0	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10 %	L1	Inicial/Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de veces en el esfuerzo 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.

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		

- 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.



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



- 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.

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		