ERICSSON

eoi escuela de negocios

ISO 27001:2005 Estudio Ericsson

Colaboración entre Ericsson y EOI Escuela de Negocios

Tutores del Proyecto:

Ignacio Retuerta y Alberto Ruíz

Presentado por:

Christy M. Galán *Jesika Reyes* *Luis A. Finol* *Luis J. Puentes*

ERICSSON

eoi escuela de negocios

Contenido

- *Descripción del proyecto*
- *Revisión del sistema de gestión de Ericsson Iberia*
- *Auditoria documental del departamento AUC (authentication office)*
- *Revisión de objetivos de control y controles*

ERICSSON

eoi escuela de negocios

DESCRIPCION DEL PROYECTO

DESCRIPCIÓN DEL PROYECTO

Ericsson Global

Ericsson MU Iberia
Unidad de Negocio

ERICSSON

eoi escuela de negocios

DESCRIPCIÓN DEL PROYECTO

Subproyectos	Propósito	Área	Entregables
1. Luis Finol: Sistema de gestión de seguridad de la información- Sistemas de Gestión	Revisa el Sistema de Gestión de Ericsson Iberia alineado a los requerimientos de la Norma ISO 27001, con la finalidad de obtener un diagnostico acerca del grado de implantación de dicha Norma para una futura Certificación.	Desarrollo Operacional	Reporte y presentación que cubra los requisitos del sistema de gestión y su conformidad con el sistema de gestión de seguridad de la información requerido por la ISO 27001.
2. Christy Galán –Luis Puentes: Auditoria documental del sistema de gestión de seguridad de la información	Evaluar la documentación del Sistema de Gestión de Seguridad de la Información del AUC () y su cumplimiento con los requisitos de la norma ISO 27001, como fase de preparación de la auditoría interna de 2009 y parte del proyecto de fin del equipo evaluador del máster de la EOI escuela de negocios.	Departamento AUC (Authentication Office)	Reporte y presentación cubriendo los hallazgos y conclusiones después de la revisión
3. Jesika Reyes: Objetivos de control y controles	Verificar el grado de implementación de los objetivos de control A8 y A13 de Ericsson Iberia (evaluación In Situ)	-Recursos Humanos -Seguridad de la información	Reporte y presentación del grado de implementación de esos controles y el análisis de las diferencias encontradas en conformidad a la ISO 27001.

ERICSSON

eoi escuela de negocios

REVISÓN DEL SISTEMA DE GESTIÓN DE ERICSSON IBERIA

ERICSSON

eoi escuela de negocios

PROPOSITO DE LA REVISÓN DEL SISTEMA DE GESTIÓN DE ERICSSON IBERIA

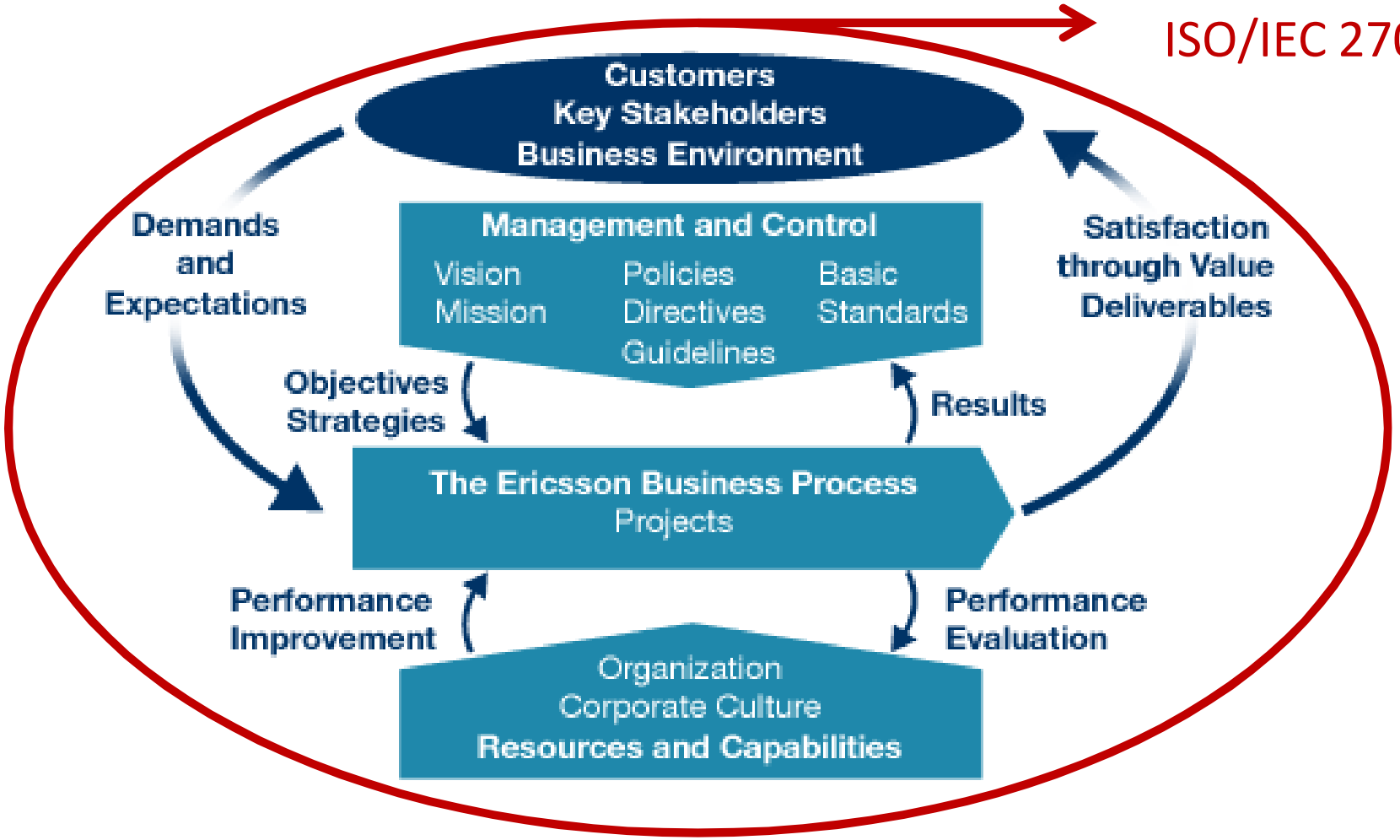
La revisión del Sistema de Gestión de Ericsson Iberia alineado a los requerimientos de la Norma ISO 27001, tiene como finalidad obtener un diagnostico acerca del grado de implantación de dicha Norma para una futura Certificación.

ERICSSON

eoi escuela de negocios

REVISÓN DEL SISTEMA DE GESTIÓN DE ERICSSON IBERIA

ISO/IEC 27001



ERICSSON

eoi escuela de negocios

REVISÓN DEL SISTEMA DE GESTIÓN DE ERICSSON IBERIA

METODOLOGÍA

ÁREAS DEL EIMS		4																	
		4.1	4.2																
			4.2.1									4.2.2							
			a	b	c	d	e	f	g	h	i	j	a	b	c	d	e	f	g	h
ÁREAS DE MEJORA																				
Control y Gestión	Visión																			
	Objetivos/ Metas y Resultados																			
	Estrategias																			
	Políticas																			
	Directivas																			
	Instrucciones																			
	Decisión Fora																			
	Estándares																			

ERICSSON

eoi escuela de negocios

REVISÓN DEL SISTEMA DE GESTIÓN DE ERICSSON IBERIA

CLASIFICACIÓN DE LAS ÁREAS DE MEJORAS

- No se encontró evidencia
- Se encuentra en el EGMS, pero no esta dentro del Iberia EGMS
- El Iberia EGMS esta preparado solo falta incluir SGSI

ERICSSON

eoi escuela de negocios

REVISÓN DEL SISTEMA DE GESTIÓN DE ERICSSON IBERIA

MEJORES PRÁCTICAS

- Política de Seguridad de la Información
- Los Objetivos de Seguridad de la Información
- Directivas de Seguridad de la Información
- Definición de Responsabilidades del SGSI
- Control de Documentos

ERICSSON

eoi escuela de negocios

AUDITORÍA DOCUMENTAL DEPARTAMENTO AUC

ERICSSON

eoi escuela de negocios

Auditoria documental del AUC

Propósito

Revisar la documentación del Sistema de gestión de Seguridad de la Información (SGSI) del AUC, como parte de la preparación de la auditoría interna del 2009 del mismo departamento y también como parte final del proyecto fin de Master en Gestión de Calidad y Excelencia Empresarial de los estudiantes de la Escuela de Negocios EOI estudiantes.

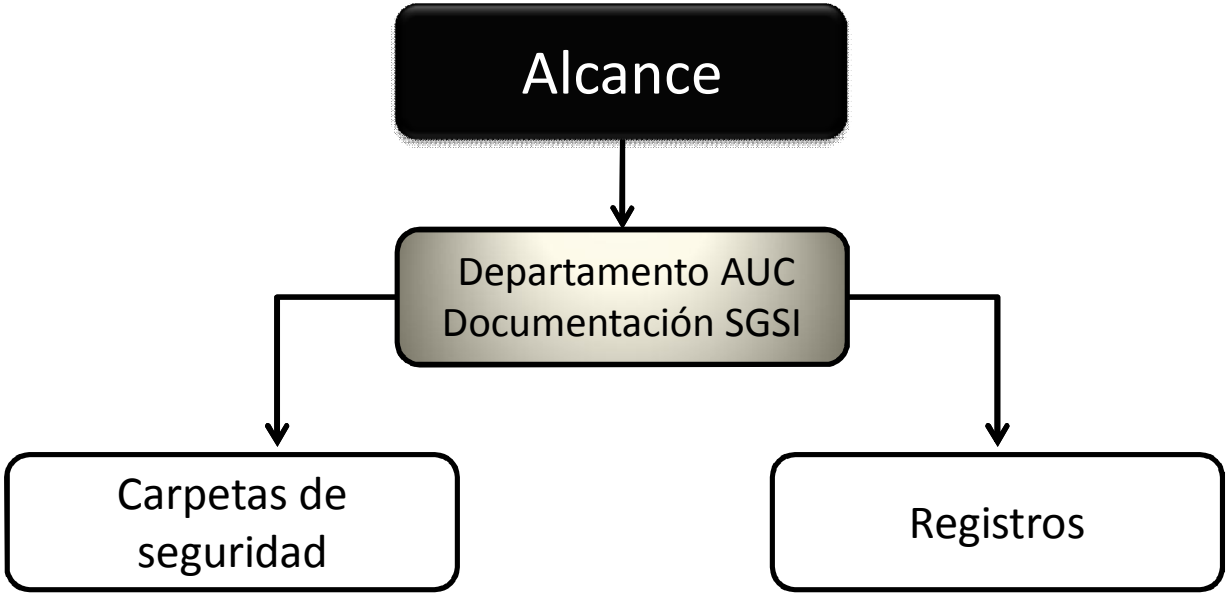
ERICSSON

eoi escuela de negocios

Auditoria documental del AUC

Alcance

El alcance de este proyecto es la documentación del sistema de gestión de seguridad de la información (SGSI) del departamento de la AUC (Authentication Office), que se ha encontrado en los siguientes folders



ERICSSON

eoi escuela de negocios

Plan auditoria documental del AUC

Semana	*Duración*	*Actividades*	*Reponsables*	*Responsables por Ericsson*
mayo 04 a 08	11:00-14:00	Declaración de aplicabilidad y revisión general de los documentos del sistema	Christy Galán/Luis José Puentes	Alberto Ruíz/Ignacio Retuerta
mayo 11 a 15	11:00-14:00	Planificación, guías y programas de formación / Documentos de SGSI	Christy Galán/Luis José Puentes	Alberto Ruiz/Ignacio Retuerta
May o 18 a 22	11:00-14:00	Prodecimientos	Christy Galán/Luis José Puentes	Alberto Ruiz/Ignacio Retuerta
Junio 1 a 5	11:00-14:00	Acciones correctivas y preventivas	Christy Galán/Luis José Puentes	Alberto Ruíz/Ignacio Retuerta
June 8 a 11	Semana completa	Elaboración de reporte	Christy Galán/Luis José Puentes	Alberto Ruíz/Ignacio Retuerta
June 12		Día de entrega	Christy Galán/Luis José Puentes	Alberto Ruíz/ Ignacio Retuerta

ERICSSON

eoi escuela de negocios

Auditoria documental del AUC

Documentos de referencia

Normas internacionales

- ISO/IEC 27001:2005
- ISO 19011:2005

Documentación de SGSI

- Sistema de gestión de seguridad de la información del departamento AUC
- Declaración de aplicabilidad ISO 27001:2005 Anexo A”
- Gestión del riesgo del AUC/reporte de analisis de riesgo 2008”
- Procedimientos y registros

ERICSSON

eoi escuela de negocios

Auditoria documental del AUC

Puntos encontrados

ERICSSON

eoi escuela de negocios

Auditoria documental del AUC

En sentido general y tomando en consideración el alcance del proyecto podemos decir que nos encontramos ante un sistema de gestión de seguridad de la información del AUC que cumple satisfactoriamente cada uno de los siguientes requerimientos de la ISO 27001:2005:

- Alcance del SGSI
- SGSI politicas y objetivos
- Procedimientos, propios y relacionados con el SGSI Gestión y operaciones
  - Medidas e Indicadores de procesos (planeación, operaciones y controles).
  - Otros procedimientos del sistema de gestión
- Documentación relacionada al análisis del riesgo:
  - -Metodología del análisis del riesgo
  - -Análisis de riesgo

ERICSSON

eoi escuela de negocios

Auditoria documental del AUC

En sentido general y tomando en consideración el alcance del proyecto podemos decir que nos encontramos ante un sistema de gestión de seguridad de la información del AUC que cumple satisfactoriamente cada uno de los siguientes requerimientos de la ISO 27001:2005:

- Documentación referente a gestión de riesgo:
  - -Procedimientos
  - -Planes
  - -Plan de Implementación de controles: riesgo y controles
- Documentos relativos a los controles in situ
- Registros que muestran la efectividad en las operaciones del SGSI
- Declaración de aplicabilidad

ERICSSON

eoi escuela de negocios

Auditoria documental del AUC

Conclusiones

En estos documentos solo se encontraron observaciones de áreas susceptibles a mejorar pero que no significan una no conformidad ni actual ni potencial para la empresa.

Para dichos puntos se realizaron las recomendaciones de lugar, pero que en sentido general son de estructura de la documentación no de no conformidades del sistema de gestión.

ERICSSON

eoi escuela de negocios

Mejores prácticas del departamento AUC

Uno de los aspectos mas sobresalientes es la disponibilidad de la información. El equipo de trabajo fue capaz de verificar y comparar informaciones sin ningún tipo de inconvenientes.

Finalmente una de las áreas mas fuertes en nuestra evaluación es toda la parte concerniente a la gestión del riesgo, resaltando que dicha gestión no es un efecto de un cumplimiento simple a una norma internacional, sino a una filosofía desarrollada para asegurar la excelencia en el sistema de gestión de seguridad de la información de Ericsson.

ERICSSON

eoi escuela de negocios

REVISIÓN OBJETIVOS DE CONTROL Y CONTROLES

ERICSSON

eoi escuela de negocios

Revisión objetivos de control y controles

Alcance

Implementación de los objetivos de control A8 y A13 de la norma ISO 27001, en los departamentos de recursos humanos y seguridad de la información de Ericsson Iberia.

ERICSSON

eoi escuela de negocios

Revisión objetivos de control y controles: documentos de referencia

Norma Internacional

ISO 27001:2005

Anexo A

Documentación SGSI

* Política de Seguridad
*Instrucción Global de Reclutamiento.
*Código de Ética
*Contrato Individual de Confidencialidad y Accesos.
*Directiva Local de acción disciplinaria y penal.
*Procedimiento de gestión de Incidentes.
*Datos estadísticos
* Otros registros
*Entrevistas

ERICSSON

eoi escuela de negocios

Revisión objetivos de control y controles (cheklist)

				Adequate			
Ref.	Control	Descripción	Required Registrations / Activities	Y	N	N/A	Notes
A.13.1.1	Reporting information security events	Information security events shall be reported through appropiate management channels as possible.	Are the Information security events reported through appropriate management channels?	X			There is a procedure and a form for this item
A.13.1.2	Reporting security weaknesses	All employess, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in system or services.	Are all users required to report any observed or suspected security weaknesses in systems or services?	X			There is a procedure, althoug many employees don´t know how act in case of a incidents.

ERICSSON

eoi escuela de negocios

Revisión objetivos de control y controles

Grado de implantación de los controles (Seguridad de los Recursos Humanos)

En sentido general, este control está implantado, si embargo, se puede mejorar, En el caso específico del control A.8.1.2, la organización debe realizar algún tipo de Revisión de antecedentes acerca de la competencias del personal.

ERICSSON

eoi escuela de negocios

Revisión objetivos de control y controles

Grado de implantación de los controles (Gestión de los incidentes de la seguridad de la información)

En el caso del control A13 la empresa lo tiene implantado correctamente, Ericsson Tiene todos los recursos necesarios para este control: política de seguridad de la Información, procesos, procedimientos e instrucciones.

ERICSSON

eoi escuela de negocios

Revisión objetivos de control y controles

Recomendaciones

Es necesario una mayor implicación de todo el personal, en algunos casos las personas no saben cómo responder a un incidente de seguridad, es decir, cómo canalizarlo. Por otra parte existe documentación que el personal desconoce y que puede ser útil en momentos cruciales. Esta situación puede causar problemas en la gestión.

ERICSSON

eoi escuela de negocios

GRACIAS!!!

Proyecto ISO 27001 Estudio Ericsson

Descripción del proyecto

El proyecto fue desarrollado como una colaboración entre EOI Escuela de Negocios y Ericsson MU Iberia. Ericsson MU Iberia es la unidad de negocio de Ericsson global que comprende España y Portugal. El proyecto consistió en analizar la alineación de diferentes ámbitos de la organización Ericsson IBERIA con algunos requisitos de la Norma ISO 27001. El proyecto inició el día 4 de Mayo del 2009 hasta el 12 de Junio del mismo año.

El alcance para la evaluación de una alineación, grado de implantación o una auditoría sería enorme e imposible de alcanzar si se hiciese para la empresa en tu totalidad, por lo que se han elegido diferentes aspectos de la ISO y su aplicación en áreas especificas.

Por el motivo mencionado anteriormente y a solicitud de la empresa se formaron tres subproyectos y cada responsable presentó a los tutores una planificación de la forma y metodología en la que se llevaría a cabo cada uno de las evaluaciones, por ejemplo: planes de auditorías, solicitud de documentación requerida, calendarización, etc. Así mismo de los días en los cuales se iba a realizar las presentaciones y entrega de los reportes con los hallazgos resultantes de dichas evaluaciones. La descripción del proyecto queda resumida en la siguiente tabla para su mejor entendimiento:

Subproyectos	Actividades	Área	Entregables
1. Luis Finol: Sistema de gestión de seguridad de la información- Sistemas de Gestión	Revisar el Sistema de Gestión de Ericsson Iberia en orden de verificar su alineación para satisfacer los requisitos de la ISO 27001	Desarrollo Operacional	Reporte y presentación que cubra los requisitos del sistema de gestión y su conformidad con el sistema de gestión de seguridad de la información requerido por la ISO 27001.
2. Christy Galán –Luis Puentes: Auditoria documental del sistema de gestión de seguridad de la información	Verificar que la documentación del SGSI de uno de los departamentos técnicos de Ericsson esta conforme según los requisitos de la ISO 27001	Departamento AUC (Authentication Office)	Reporte y presentación cubriendo los hallazgos y conclusiones después de la revisión
3. Jesika Reyes: Objetivos de control y controles	Verificar el grado de implementación de los objetivos de control A8 y A13 de Ericsson Iberia (evaluación In Situ)	-Recursos Humanos -Seguridad de la información	Reporte y presentación del grado de implementación de esos controles y el análisis de las diferencias encontradas en conformidad a la ISO 27001.

Objetivo General

El propósito del proyecto es tener una visión general de la aplicación real de la Norma ISO 27001 en una empresa.

Objetivos Específicos

Tal como se expresó anteriormente el proyecto fue dividido en tres subproyectos y para cada uno de ellos se plantearon objetivos específicos, tales como los siguientes:

- realizar una revisión de los controles A8 y A13 de la ISO 27001, para verificar su grado de implantación en la empresa.

- Evaluar la documentación del Sistema de Gestión de Seguridad de la Información del AUC () y su cumplimiento con los requisitos de la norma ISO 27001, como fase de preparación de la auditoría interna de 2009 y parte del proyecto de fin del equipo evaluador del máster de la EOI escuela de negocios.

- Revisa el Sistema de Gestión de Ericsson Iberia alineado a los requerimientos de la Norma ISO 27001, con la finalidad de obtener un diagnostico acerca del grado de implantación de dicha Norma para una futura Certificación.

Subproyectos

Luego de realizar las evaluaciones cada responsable presentó y entregó su reporte con las conclusiones y hallazgos encontrados, se identificaron además mejores prácticas, puntos susceptibles de mejorar y algunas recomendaciones igualmente fueron presentadas. A continuación se presenta una visión general del despliegue de reporte de cada subproyecto.

Subproyecto 1: Sistema de gestión de seguridad de la información- Sistema de Gestión

Alcance

Revisión del Sistema de Gestión de Ericsson Ibera para poder tener una retroalimentación de cómo se encuentra el Sistema de Gestión de Iberia en comparación con los requerimientos de la Norma ISO ISO/IEC 27001, Esta Revisión solo Engloba al Sistema de Gestión de Ericsson Iberia se descarta el Sistema de Gestión del Grupo Ericsson.

Documentación de referencia

- Norma internacional: ISO/IEC 27001:2005
- Sistema de Gestión de Ericsson Iberia

Hallazgos

La revisión del Sistema de Gestión de Ericsson Iberia se llevo a cabo por medio de una matriz de comparación en la cual se cruzaban las áreas del Sistema de Gestión de Ericsson Iberia con los requerimientos de la Noma ISO/IEC 27001.

Dentro de esta revisión se observaron áreas susceptibles a mejorar ya que se observó documentación que:

- Se encuentra dentro del Sistema de Gestión del Grupo Ericsson pero no en el Sistema de Gestión de Ericsson Iberia.
- Se encuentra dentro del Sistema de Gestión de Ericsson Iberia pero no hace referencia al Sistema de Gestión de la Seguridad de la Información.

Al igual que se observó documentación la cual estaba completamente implantada acordes a los requerimientos de la Norma ISO/IEC 27001.

Mejores prácticas

Ericsson posees un sólido e integrado sistema de gestión, el cual ha sido aprobado por la alta gerencia, este sistema de gestión contiene diversos aspectos como son: los estándares internacionales ISO 9001, ISO 14001 and ISO/IEC 27001. El Sistema de Gestión de Iberia posee unas políticas muy bien definidas, objetivos e instrucciones de trabajos relacionadas con confidencialidad, integridad y disponibilidad sumada a la definición de las responsabilidades de acuerdo a los requisitos de la Norma ISO/27001.

Conclusión

Según lo que se pudo observar durante la revisión se puede concluir que en general y tomando en cuenta el alcance del subproyecto, Ericsson Iberia posee in Sistema de Gestión completamente integrado, actualizado, sin embargo posee ciertas áreas de mejoras que se puede atacar de una manera fácil y rápida para poder cumple en plenitud con los requerimientos de la Norma ISO 27001 y poder acceder a la certificación de todo el Sistema de Gestión de Ericsson Iberia.

Subproyecto 2: Auditoria documental departamento AUC (authentication office)

Alcance

El alcance es la documentación del sistema de gestión de seguridad de la información (SGSI) del departamento de la AUC (Authentication Office)

Documentación de referencia

- Normas internacionales: ISO/IEC 27001:2005 e ISO 19011:2005
- Documentación de sistema de gestión de seguridad de la información (SGSI): Documento de SGSI del departamento AUC, declaración de aplicabilidad, gestión y análisis de riegos, procedimientos y registros, todos estos actualizados a fechas recientes.

Hallazgos

La revisión de la documentación se dividió en 2 partes: la documentación de sistema de gestión de la seguridad de la información y la declaración de aplicabilidad.

En estos documentos solo se encontraron observaciones de áreas susceptibles a mejorar pero que no significan una no conformidad para la empresa, por ejemplo actualizaciones de enlaces, sustitución de un por otro, arreglos de nomenclaturas en la documentación del sistema, puntos para los cuales se realizaron las recomendaciones de lugar, pero que en sentido general son de estructura de la documentación no de no conformidades del sistema de gestión.

Mejores prácticas

Uno de los aspectos más sobresalientes es la disponibilidad de la información. El equipo de trabajo fue capaz de verificar y comparar informaciones sin ningún tipo de inconvenientes.

Finalmente una de las áreas más fuertes en nuestra evaluación es toda la parte concerniente a la gestión del riesgo, resaltando que dicha gestión no es un efecto de un cumplimiento simple a una norma internacional, sino a una filosofía desarrollada para asegurar la excelencia en el sistema de gestión de seguridad de la información de Ericsson.

Conclusión

Según lo anteriormente dicho pudimos concluir que en sentido general y tomando en consideración el alcance del subproyecto, el sistema de gestión de seguridad de la información del AUC, cumple satisfactoriamente cada uno de los requerimientos de la ISO 27001:2005.

Subproyecto 3: Objetivos de control y controles

Alcance

Implementación de los objetivos de control A8 y A13 en los departamentos de recursos humanos y seguridad de la información de Ericsson Iberia.

Documentación de referencia

- Normas internacionales: ISO/IEC 27001:2005 e ISO 19011:2005
- Documentación del sistema: Políticas de seguridad, instrucciones globales de reclutamiento, código de ética, acuerdo de confidencialidad y accesos, directiva local de acción disciplinaria y penal, procedimientos, entrevistas a empleados.

Hallazgos

En sentido general, estos controles están implantados satisfactoriamente en conformidad a la norma en cuestión, sin embargo, se puede mejorar, en el caso específico de un control en específico en el cual la organización debe realizar algún tipo de revisión de antecedentes acerca de las competencias del personal.

Conclusión

Luego de haber entrevistado además algunos empleados se llegó a la conclusión de que es necesario una mayor implicación de todo el personal ya que en algunos casos las personas no saben cómo responder a un incidente de seguridad, es decir, cómo canalizarlo. Por otra parte existe documentación que el personal desconoce y que puede ser útil en momentos cruciales. Esta situación puede causar problemas en su gestión.