"Inteligencia, al servicio de la confianza"

4301 – 1 ANEXO INFORMACIÓN ADICIONAL ISO 27001:2013

Versión 2.0 / 01.Agosto.2017

Estructura de la Organización, incluyendo número de empleados para cada función	
Describa si tiene alguna documentación relacionada con el SGSI que no pueda estar disponible para revisión del Equipo Auditor (tales como registros del SGSI o información sobre el diseño y la eficacia de los controles) por contener información sensible o confidencial. *Nota: En caso afirmativo Cotecna evaluará la necesidad de comunicar al cliente que la auditoría de certificación no puede tener lugar hasta que se otorguen los acuerdos de acceso apropiados.*	
Por favor proporcione el Compromiso de Aplicabilidad (SOA)	
Describa a un Alto nivel la estructura de la Organización (ej: Junta, MD/CEO, Reportes Directos) y descripción de cargos/funciones. Describa a un Alto nivel la estructura de la Organización las áreas claves del negocio (ej: Grupo TIC, Ventas y Mercadeo, Servicios, Manufactura, etc) descripción de cargos/funciones.	
Declarar las exclusiones de controles aplicables (Si aplicara)	
¿Qué información es protegida?	
Para cada categoría detalle información que debe protegerse y una breve descripción de por qué esta información se ha de proteger. • Información • Software • Física • Servicios • Gente • Intangibles (ej: Goodwill)	
¿Ha realizado usted una evaluación de riesgo dentro del alcance definido para la certificación?	
Sírvase facilitar detalles de cuando se completó la evaluación de riesgos y si es posible relacione los 5 primeros riesgos identificados?	
¿Qué estrategias de reducción de riesgos se encuentran actualmente en marcha para gestionar los riesgos identificados?	
¿Con qué frecuencia la política de riesgos es revisada y / o actualizada?	
¿La auditoría interna de seguridad se completó dentro del ámbito del SGSI (sistema de Gestión de Seguridad de la Información)?	
¿Cuándo se realizó la última Auditoria?	
Describa brevemente los hallazgos de esa auditoria	
Cuando se realizó la última revisión por la dirección en el ámbito del alcance del SGSI?	
Nota: El organismo de certificación no certificará un SGSI a menos que haya sido realizada al menos una Revisión por la dirección y una auditoría interna del SGSI con cubrimiento al alcance de la certificación.	

Número de Sitios	
¿Cuál es el alcance geográfico de su organización?	
¿Cuantos sitios físicos están incluidos en el alcance del SGSI (sistema de Gestión de Seguridad Informática)?	
Para cada locación por favor proporcione el número de empleados y principales funciones realizadas en esas locaciones.	
Proporcione detalles de los activos de información almacenados en esos lugares.	
Tráfico de Datos entre Sitios y Arquitectura Técnica	
Proporcione en alto nivel la infraestructura de la red para su organización?	
Proporciona descripción de los volúmenes de tráfico y los tipos de tráfico entre las distintas localidades?	
Que controles de seguridad existen en el sitio y el tráfico de datos?	
Sírvase proporcionar detalles sobre el hardware y software que constituye la infraestructura crítica de su entorno? Esto debe incluir intranet, entre el sitio y el mundo externo.	Numero de sistemas de información (aplicaciones) que soportan directamente las actividades consideradas en el alcance: Número de equipos servidores, y equipos activos de la red y de seguridad en ambientes de desarrollo y producción. Incluya las máquinas virtuales, no incluya las máquinas de contingencia o pruebas: El alcance incluye actividades de comercio electrónico? Se realizan transacciones electrónicas? Se permite el acceso remoto, móvil y/o inalámbrico desde equipos controlados por la organización? Se permite el acceso remoto, móvil y/o inalámbrico desde equipos NO controlados por la organización (personales o de terceros)?
¿Qué tipos de acceso externo se permiten para su entorno de red? Considere la posibilidad de conexiones desde el personal que trabaja en el campo, los clientes, socios comerciales etc.	
¿Hay riesgos específicos que deben considerarse a través de permitir el acceso externo a sus redes? En caso afirmativo indique los detalles.	
Normas y Regulaciones Aplicables	
Proporcione detalles de reglamentación y / o normas jurídicas que su organización está obligada a cumplir.	
¿Su organización necesita satisfacer alguna obligación contractual o acuerdos de nivel de servicio? Si es así, por favor Proporcione detalles	
¿Puede usted aportar pruebas de cumplimiento de las normas aplicables y reglamentos?	
Seguridad Organizacional	

Un oficial de seguridad ha sido nombrado?	
¿Existe un marco de Control para la gestión de la seguridad dentro de la organización? En caso afirmativo dar detalles.	
¿Qué otros sistemas de seguridad y los controles tiene usted en su lugar?	

Razón Social:

Por favor marcar la complejidad (baja, media o alta)

Factores	**Calificación de los Factores**		
	Baja	**Media**	**Alta**
a) Complejidad del SGSI * Requisitos de Confidencialidad-Integridad-Disponibilidad (CIA) * Número de activos críticos * Número de procesos y servicios	* Poca información sensible o confidencial, bajos requisitos de disponibilidad * Pocos activos críticos (en términos de CIA) * Un único proceso de negocio con pocas interfases y pocas unidades de negocios involucradas	* Altos requisitos de disponibilidad o alguna información sensible / confidencial * Algunos activos críticos * 2-3 procesos sencillos de negocios con pocas interfases y pocas unidades de negocio involucradas	* Alta cantidad de información sensible o confidencial (salud, información de identificación personal, seguros, bancaria) o altos requisitos de disponibilidad * Muchos activos críticos * Más de 2 procesos complejos con muchas interfases y unidades de negocio involucradas
Marque X en el que le corresponda	☐	☐	☐
b) El / (los) tipo (s) de negocio desarrollados dentro del alcance del SGSI	* Negocios de bajo riesgo sin requisitos regulatorios	* Altos requisitos regulatorios	* Negocios de alto riesgo con solo requisitos regulatorios limitados
Marque X en el que le corresponda	☐	☐	☐
c) Desempeño previo demostrado del SGSI	* Certificado recientemente * No certificado aún, pero el SGSI está totalmente implementado, con muchas auditorias y ciclos de mejoramiento, incluyendo auditorías internas documentadas, revisiones gerenciales y eficaz mejora continua del sistema.	* Reciente auditoria de seguimiento * No certificado pero el SGSI parcialmente implementado. Algunos controles del sistema de gestión disponibles e implementados, algunos procesos con mejora continua pero parcialmente documentados.	* Sin certificación ni auditorias recientes * El SGSI es nuevo y no está establecido totalmente (retraso en mecanismos de control específicos del sistema de gestión, procesos inmaduros de mejoramiento continuo, ejecución de procesos no repetitivos)

Marque X en el que le corresponda	☐	☐	☐
d) Tamaño y diversidad de tecnología utilizada en la implementación de los componentes del SGSI (ejemplo: número de diferentes plataformas de TI, número de redes separadas)	* Ambiente altamente estandarizado (pocas plataformas de TI, servidores, sistemas operativos, bases de datos, redes, etc.)	* Estandarizadas pero diversas plataformas de TI, servidores, sistemas operativos, bases de datos, redes.	* Alta diversidad y complejidad de TI (ejemplo: muchos diferentes segmentos de red, tipos de servidores o bases de datos, número de aplicaciones claves)
Marque X en el que le corresponda	☐	☐	☐
e) Tamaño de contratación y acuerdos de terceras ´partes usados dentro del alcance del SGSI	* Sin contratación y baja dependencia con proveedores, o * Acuerdos de contratación bien definidos, gestionados y monitoreados * Los contratantes tercerizados tienen certificación SGSI * Informes disponibles sobre la independencia de los contratistas	* Muchos contratos tercerizados gestionados parcialmente	* Alta dependencia de contratos tercerizados o proveedores con gran impacto sobre las actividades del negocio, o * Desconocimiento del total o tamaño de contratos * Muchos contratos tercerizados sin gestión
Marque X en el que le corresponda	☐	☐	☐
f) Tamaño del desarrollo de sistemas de información	* No hay desarrollo de sistemas in-house * Uso de plataformas de software estandarizadas	* Uso de plataformas estandarizadas de software con compleja parametrización/configuración * Alto software personalizado * Algunas actividades de desarrollo in-house o contratado	* Altas actividades de desarrollo de software interno con muchos proyectos en curso para propósitos del negocio
Marque X en el que le corresponda	☐	☐	☐

g) Número de sitios y número de sitios para DR (Recuperación de desastres)	* Bajo requerimientos de disponibilidad o uno o ningún sitio alternativo para DR	* Medios o altos requerimientos de disponibilidad y uno o ningún sitio alternativo para DR	* Altos requisitos de disponibilidad (servicios 24/7) * Muchos sitios alternativos para DR * Muchos Data Centers
Marque X en el que le corresponda	☐	☐	☐
h) Para auditoria de re-certificación o seguimiento: la cantidad y tamaño de los cambios relevantes al SGSI de acuerdo a ISO/IEC 17021-1. 8.5.3	* Sin cambios desde la última auditoría de re-certificación	* Cambios menores en el alcance o la (Declaración de Estabilidad) del SGSI (ejemplo: algunas políticas, documentos, etc) * Cambios menores en los factores anteriores	* Cambios grandes en el alcance o la (Declaración de Estabilidad) del SGSI (nuevos procesos, nuevas unidades de negocios, áreas, metodologías para la gestión de valoración de riesgos, políticas, documentos, tratamiento de riesgos) * Cambios grandes en los factores anteriores
Marque X en el que le corresponda	**N/A** ☐	☐	☐