TOPCERTIFIER
www.topcertifier.com

METODOLOGÍA DEL SERVICIO ISO 27001:2013

INFORMACIÓN GESTIÓN DE SEGURIDAD SISTEMA (SGSI)

TOPCERTIFIER
www.topcertifier.com

INTRODUCCIÓN A ISO 27001:2013

ISO 27001:2013 permite a una organización identificar riesgos de seguridad de la información. Tener en cuenta las amenazas, las vulnerabilidades, los impactos y proteger la organización. sin comprometer su CIA (Disponibilidad de Integridad y Confidencialidad) de información mediante la adopción Sistema de gestión de seguridad de la información adecuado La agenda general de ISO 27001:2013 es cubrir los siguientes aspectos.

- Proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información con controles físicos y técnicos.

- Garantizar que los SGSI estén integrados en los procesos de negocio de las organizaciones.

- Crear una cultura organizacional que fomente la participación activa de los empleados en el Sistema de Gestión de Seguridad de la Información.

PATADA INICIAL

La reunión inicial es una herramienta esencial para comunicar y planificar la ejecución del proyecto. con obstrucción mínima y para completar el proyecto dentro del tiempo y costo planificados. La agenda de la reunión inicial es:

- Discusión del plan del proyecto: Esto incluye discusión sobre la rendición de cuentas y la responsabilidad de los interesados. titulares. hitos y entregables del proyecto

- Alcance de los servicios y alcance de la certificación

- Requisitos legales y reglamentarios

CREACIÓN DEL EQUIPO CENTRAL

- Nombramiento del CISO
- Designación del Comité de Gestión de Seguridad de la Información
- Designación de Auditores Internos
- Gerente de BCP
- Nombramiento del Líder ISO

TOPCERTIFIER
www.topcertifier.com

ANÁLISIS DE BRECHAS

Durante esta fase, llevamos a cabo un análisis de brechas para verificar qué parte de sus prácticas actuales están en en línea con los requisitos estándar. Las prácticas se verifican según estos cuatro criterios de referencia.

- Requisitos de la norma ISO 27001:2013
- SOA
- Requisitos legales, estatutarios y reglamentarios
- Requisitos del cliente
- Políticas y procedimientos internos

Los resultados de este análisis se presentan en forma de Informe de análisis de brechas. Este informe actúa como la lista de elementos de acción para el recordatorio del proyecto.

FORMACIÓN DE CONCIENTIZACIÓN SOBRE ISMS

Se llevará a cabo una capacitación de concientización sobre el SGSI a los empleados de su organización. el entrenamiento La sesión tiene como objetivo ayudar a los empleados a adquirir conocimientos, comprender los conceptos de ISO 27001:2013, y alinear procesos y prácticas para lograr un entorno de trabajo seguro y libre de amenazas. Cuando el personal ha sido capacitado, puede pensar, actuar y contribuir a lograr los objetivos. objetivos.

REGISTRO DE RIESGOS Y SOA

Se documentará un procedimiento de gestión de riesgos y se utilizará como referencia para gestionar la riesgos identificados en consulta con todos los propietarios de procesos y jefes funcionales. Usamos ISO 31000 & Técnicas estándar de gestión de riesgos ISO 27005 para identificar, analizar, evaluar, documentar, priorizar, tratar y cuantificar los riesgos identificados. Este paso crea un Registro de Riesgos. Riesgo adecuado Los planes de tratamiento se identifican en función del nivel de apetito de riesgo y el factor CIA de la empresa. Los resultados de dichas acciones se calculan, registran, evalúan y documentan. El La Declaración de Aplicabilidad (SOA) define e identifica los controles físicos y técnicos aplicable a su organización en función de sus procesos y requisitos comerciales.

TOPCERTIFIER
www.topcertifier.com

GESTIÓN DE ACTIVOS

Ayudamos a desarrollar políticas y procedimientos de gestión de activos coordinando con el cabezas funcionales y comprensión sobre el proceso. El principal objetivo del activo.
la gestión es:

- Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.

- Para evitar la divulgación, modificación, eliminación o destrucción no autorizada de la información almacenada en los medios

- Garantizar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organizacion

SEGURIDAD DE RED/COMUNICACIONES:

Ayudamos a desarrollar políticas y procedimientos de gestión de seguridad de la red coordinando con los jefes funcionales y comprensión sobre el proceso.
El principal objetivo de la seguridad de la red es:

- Garantizar la protección de la información en las redes y su procesamiento de información de soporte. instalaciones

- Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa

GESTIÓN DE INCIDENTES

Ayudamos a desarrollar políticas y procedimientos de gestión de incidentes coordinando con el cabezas funcionales y comprensión sobre el proceso. El principal objetivo del incidente.
la gestión es:

- Garantizar un enfoque coherente y eficaz para la gestión de la seguridad de la información. incidentes, incluida la comunicación sobre eventos y debilidades de seguridad

TOPCERTIFIER
www.topcertifier.com

GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Ayudamos a desarrollar políticas y procedimientos de gestión de la Continuidad del Negocio mediante Coordinación con los jefes funcionales y comprensión del proceso. El objetivo principal de gestión de la continuidad del negocio es el siguiente:

- Para garantizar que la continuidad de la seguridad de la información esté integrada en el negocio de la organización. sistemas de gestión de continuidad

- Garantizar la disponibilidad de instalaciones de procesamiento de información.

SEGURIDAD FÍSICA:

Ayudamos a desarrollar políticas y procedimientos de seguridad física coordinando con el cabezas funcionales y comprensión sobre el proceso. El objetivo principal de Física la seguridad es:

- Para evitar el acceso físico no autorizado, daños e interferencias a la actividad de la organización. instalaciones de información y procesamiento de información

- Para evitar pérdidas, daños, robo o compromiso de activos e interrupción del funcionamiento de la organización. operaciones

SEGURIDAD DE RECURSOS HUMANOS:

Ayudamos en el desarrollo de políticas y procedimientos de RR.HH. coordinándonos con los jefes funcionales. y comprensión sobre el proceso. El principal objetivo de la seguridad de RRHH es:

- Garantizar que los empleados y contratistas comprendan sus responsabilidades y sean aptos para los roles para los cuales son considerados

- Para proteger los intereses de la organización como parte del proceso de cambio o terminación empleo

- Asegurar que se haya brindado la capacitación adecuada a todos los empleados y proveedores conrespeto a la seguridad de la información

TOPCERTIFIER
www.topcertifier.com

DOCUMENTACIÓN

Nuestros expertos enumerarán las políticas, procesos, SOP, SOA aplicables y registros que deben ser definido y documentado según los requisitos de ISO 27001:2013 discutiendo con cada uno Jefes de departamento y funciones le ayudamos en la creación de la documentación necesaria.

ESTABLECER CONTROLES ISMS

Una vez que las políticas, procesos, Declaración de Aplicabilidad (SOA), sus controles y SOP se hayan Se ha documentado y se ha enumerado la lista de registros que se recopilarán y se ha incluido al personal. identificados y capacitados en tales actividades, entonces la necesidad es operar, monitorear y revisar las eficiencias de tales procesos.

FORMACIÓN DEL AUDITOR INTERNO

Se brindará capacitación de Auditor Interno (IA) ISO 27001:2013 al personal identificado. Esta capacitación equipará a dicho personal para analizar la necesidad de IA, planificar y programar la IA, preparar listas de verificación de auditoría y realizar una evaluación de impacto (IA) y documentar e informar sus observaciones al nivel superior. gestión.

AUDITORÍA INTERNA

Nuestros expertos supervisarán la realización de la auditoría interna por parte de su equipo de auditoría interna. Esta auditoría interna identificará las brechas aún existentes en el sistema y demostrará el nivel de preparación para afrontar la auditoría de certificación. Esta auditoría le da a la organización la oportunidad de identificar y rectificar todas las no conformidades antes de proceder a la auditoría de certificación. la cimaLa dirección está informada de los resultados de la auditoría interna.

TOPCERTIFIER
www.topcertifier.com

ANÁLISIS DE CAUSA RAÍZ (RCA) Y ACCIONES CORRECTIVAS

Todas las no conformidades identificadas durante la auditoría interna, auditorías de clientes o de terceros, o de Metodología de evaluación y tratamiento de riesgos, registro de riesgos Registro de Incidentes, Vulnerabilidad Informe de prueba de evaluación y penetración (VAPT), ataques de malware, registro de tiempo de inactividad, red cuestiones, controles de acceso, registro de activos, informes de evaluación de riesgos de tereros, información de la CIA Se deben enumerar la clasificación, los ataques internos y externos y cualquier otra fuente. RCA para ser realizado utilizando técnicas como los métodos Brainstorming y Fish-Bone. El correctivo óptimo se implementan acciones. La eficacia de dichas acciones se documenta y revisa a través de un Informe de acciones correctivas (CAR).

REUNIÓN DE REVISIÓN DE LA ADMINISTRACIÓN (MRM)

El MRM es una oportunidad para que todas las partes interesadas del SGSI se reúnan en intervalos programados para revisar, discutir y planificar acciones sobre los siguientes puntos de la agenda.

- Efectividad del Sistema de Gestión actual respecto al SGSI
- Planes y registros de evaluación de riesgos y tratamiento de riesgos.
- Resultados sobre CIA (Confidencialidad, Integridad y Disponibilidad) de la información
- Hallazgos de auditoría y no conformidades de todas las fuentes.
- Plan de acción correctiva para resolver cualquier elemento abierto
- Mejoras continuas realizadas al sistema.
- Recursos y capacitaciones requeridas
- Aspectos estatutarios y de cumplimiento

AUDITORÍA DE CERTIFICACIÓN: ETAPA 1

Cuando el nivel de preparación haya alcanzado niveles adecuados, el proceso de certificación comienza. Un auditor designado por el Organismo de Certificación (OC) verifica la Norma requisitos a través de una auditoría de etapa 1. Esto implica que el auditor revise las políticas, procesos, SOPs, SOA, registros operativos críticos, registros IA y MRM. Cualquier desviación importante de los CB Las expectativas serán notificadas en este punto para introducir las correcciones necesarias. Esto reduce las posibilidades de que se produzcan no conformidades importantes durante la auditoría de certificación. El Certificador TOP actuará como enlace con todas las partes interesadas y supervisar la finalización sin problemas de la auditoría.

TOPCERTIFIER
www.topcertifier.com

AUDITORÍA DE CERTIFICACIÓN: ETAPA 2

Al completar con éxito la auditoría de la Etapa 1, el auditor se centra en una auditoría detallada del informe y documentación del Sistema de Gestión de Seguridad de la Información de la organización. TOPCertifier habría capacitado a su personal sobre los requisitos de auditoría y con confianza frente a la auditoría. Nuestros expertos estarán presentes para ayudar en cualquier medio necesario para el buen funcionamiento. funcionamiento de la auditoría. TOPCertifier ayudará a su equipo a cerrar cualquier no conformidad identificados durante la auditoría. Al completar con éxito la auditoría de certificación, TOPCertifier se comunicará con todas las partes interesadas para redactar, aprobar y publicar el certificado final.

CONTINUACIÓN DEL CUMPLIMIENTO

TOPCertifier será parte del proceso de cumplimiento de su organización y lo ayudará periódicamente Intervalos con capacitaciones necesarias, soporte y actualizaciones del sistema, auditorías internas y externas. y renovación periódica de su certificación.