LA

SEGURIDAD

DE LA

INFORMACIÓN

DEPENDE

DE TODOS

TERMINOS Y DEFINICIONES.

Aprendamos nueves términos y definiciones que nos permitirán unificar conceptos frente al Subsistema de Seguridad de la Información.

¿QUÉ ES SEGURIDAD DE LA INFORMACIÓN?

La preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio (ISO 17799).

DISPONIBILIDAD

Vinculado con la seguridad de la información se refiere a la propiedad de ser accesible y utilizable por una entidad autorizada.

CONFIDENCIALIDAD

La propiedad vinculada con la seguridad de la información por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.

EVENTO DE SEGURIDAD DE LA INFORMAACIÓN

La ocurrencia detectada en un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas o una situación desconocida hasta el momento y que puede ser relevante para la seguridad de la información.

INCIDENTE DE SEGURIDDAD DE LA INFORMACIÓN

Un único evento o una serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones empresariales y de amenazar la seguridad de la información.

SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI).

La parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión de la seguridad de la información o SGSI incluye la estructura organizativa. las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos. Puede seguir los requisitos de la norma ISO 27001.

INTEGRIDAD

La propiedad de salvaguardar la exactitud y completitud de los activos.

RIESGO RESIDUAL

Riesgo remanente que existe después de que se hayan tornado las medidas de seguridad.

ACEPTACIÓN DE RIESGO

La decisión de aceptar un riesgo en la seguridad de la información.

ANÁLISIS DE RIESGO

Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos en la seguridad de la información.

EVALUACIÓN DE RIESGO

El proceso general de análisis y estimación de los riesgos en la seguridad de la información.

ESTIMACIÓN DE RIESGOS

El proceso de comparación del riesgo en la seguridad de la información estimado con los criterios de riesgo, para así determinar la importancia del riesgo en la seguridad de la información.

GESTION DE RIESGOS

Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos de la seguridad de la información.

TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El proceso de selección e implementación de las medidas encaminadas a modificar los riesgos de la seguridad de la información.

DECLARACIÓN DE APLICABILIDAD

Declaración documentada que describe los objetivos de control y los controles que son relevantes para el Sistema de Gestión de la Seguridad de la Información o SGSI de la organización y

aplicables al mismo. Los controles del Sistema de Gestión de Seguridad de la Información o SGSI se basan en los resultados de la evaluación de riesgos de seguridad de la información (requisitos legales o reglamentarios, obligaciones contractuales y las necesidades de la organización en materia de seguridad de la información).

IMPLEMENTANDO EL SISTEMA DE SEGURIDAD DE LA INFORMCIÓN EN LA TERMINAL DE TRANSPORTE S.A.

¿Qué es la ISO 27001?

ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.

La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002.

PLANEAR (establecer el SGSI): Establecer políticas, objetivos, metas, procesos y procedimientos relevantes para gestionar los riesgos y mejorar la seguridad de la información en los sistemas de información y su alineamiento con las políticas y objetivos de la organización.

PLANEAR

Documentación – Caracterización de los procesos.

Definición del alcance SGSI

Definición de la Política de Seguridad

HACER (Implementar y Operar el SGSI): Implementar y colocar en operación las políticas, controles, procesos y procedimientos de seguridad de la información.

HACER

Procedimiento documentado de la documentación, aprobación y control de los documentos del SGSI

Certificación de las sesiones de entrenamiento y sensibilización realizadas para el GSI.

Guías de Autocontrol con la asignación de responsables de ejecutar y supervisar los controles

VERIFICAR (Monitorear, medir y revisar el SGSI): Evaluar y donde sea aplicable, medir el desempeño del proceso contra la política de seguridad, los objetivos y la experiencia práctica, y reportar los resultados a la Gerencia para su revisión.

VERIFICAR

Guías y procedimientos de monitoreo y medición periódica de la seguridad existente y el riesgo residual.

Modelo de organización de la función de seguridad en los Servicios de Tecnología de Información de la Empresa.

ACTUAR (Mantener y mejorar continuamente el SGSI): Ejercer las acciones correctivas y preventivas, basados en los resultados de las revisiones gerenciales, para a lograr el mejoramiento continuo del SGSI.

ACTUAR.

Procedimiento de mejoramiento continúo.

En qué consiste la certificación en iso 27001?

El SGSI basado en ISO/IEC 27001 permite la gestión y control de los riesgos de la seguridad de la información en las organizaciones para las cuales la información y la tecnología son activos importantes de su negocio.

Mediante las mejores prácticas de seguridad de la información, las organizaciones que certifican su SGSI demuestran ante sus accionistas, clientes, autoridades, proveedores y demás partes interesadas, la debida diligencia en este importante aspecto y garantizan la aplicación adecuada de los recursos en las áreas de mayor impacto potencial, optimizando así sus inversiones y costos de seguridad.

¿A quiénes está dirigida?

- Empresas de servicios.
- Prestadores de servicios tercerizados
- Empresas del sector financiero de banca y seguros.
- Empresas del sector de tecnología de la información.
- Empresas de comunicaciones.
- Empresas de seguridad y custodia.
- Entidades públicas.

Todo tipo de empresas de cualquier sector económico o industrial, públicas o privadas que hagan uso intensivo de la tecnología de la información.

¿Qué beneficios trae su implementación?

- Habilita y potencializa el uso de las más actuales herramientas de colaboración y de gestión de la información, protegiendo el valor de la confidencialidad, la integridad y la disponibilidad de la información para el negocio.

- La implementación del sistema de gestión de seguridad de la información se constituye en una herramienta para la comunicación eficaz entre la alta dirección empresarial, los responsables de la gestión y custodia de la información y los clientes y demás interesados.

- Previene y reduce eficazmente el nivel de riesgo, mediante la implantación de los controles adecuados; de este modo, prepara a la organización ante posibles emergencias y garantiza la continuidad del negocio.

- Permite a la dirección monitorear, evaluar, asignar y gestionar los recursos necesarios para la seguridad de la información. Incrementa el nivel de conciencia del personal respecto a los tópicos de seguridad de la información

SC-CER325129
CO- SC-CER325129

SI-CER330392
CO- SI-CER330392