Publicado en Madrid el 13/07/2020

ISO 27001 se convierte en una herramienta de ciberprotección para los momentos de crisis por la COVID - 19

Una vez decretado el estado de alarma por la COVID-19, y de que las actividades presenciales de las empresas tuvieran que verse afectadas; muchas de ellas continuaron sus actividades mediante teletrabajo y herramientas de conexión online que les permitieran seguir con sus actividades laborales. La norma ISO 27001 ha sido una ventaja para todas ellas

Las empresas han tenido que asegurar que sus actividades se realizasen bajo estándares de seguridad para no comprometer la integridad, la disponibilidad y la confidencialidad de la información gestionada entre empleados, clientes y proveedores. Es por ello que se han tenido que revisar los protocolos de seguridad de la información e incurrir en gastos adicionales con el objetivo de tener todas las garantías necesarias para seguir trabajando de manera online sin preocuparse de ciberataques o problemas de pérdidas de información o robo de la misma.

Muchas organizaciones ya contaban con ventaja al tener implantada la Norma ISO 27001 por lo que han logrado ver todos sus beneficios; dado que esta norma contempla los protocolos de trabajo seguro y proporciona las herramientas necesarias para que las empresas, sus clientes y sus proveedores actúen de manera segura y con todas las garantías en la seguridad de la información.

¿Qué proporciona la ISO 27001: Seguridad de la Información?
Si ISO 27001 era una norma en crecimiento, ahora va a ser una norma en crecimiento exponencial por los nuevos tiempos que esperan una vez sufrida esta pandemia. Se puede afirmar que tras la COVID-19 muchas empresas se encontraron con sus verdaderos fallos en el uso de la información y de la seguridad de la misma.

Algunos de los principales problemas encontrados han sido:

Seguridad de los equipos

Copias de seguridad

Intercambio de información

Control de acceso a la red

Ordenadores portátiles y comunicaciones móviles

Teletrabajo

Gestión de claves

Protección de datos y privacidad de la información de carácter personal

Planes de continuidad de negocio

Estos problemas que han encontrado muchas empresas a raíz del teletrabajo, son algunos de los controles que establece ISO 27001 y que las empresas que ya está certificadas tienen implementados y por lo tanto bajo control.

Por eso su transición al teletrabajo o a otra nueva forma de operar ha sido sencilla y rápida y sus conocimientos de la norma los han conducido a un escenario más amplio y mejor actualmente.

Gestionar los riesgos con la Norma ISO 27001
Al tener implantada la Norma de seguridad de la información se podrá hacer una evaluación de los posibles riesgos y de los posibles puntos débiles que posee la empresa.

Con la aparición de la pandemia la cantidad de información malintencionada que circula por los diferentes medios de comunicación digital sobre el CORONAVIRUS hace más sensible el tratamiento de la información y es por ello que se hace imperativo mantener resguardada la información y establecer los protocolos de seguridad dentro de la compañía.

Con la implantación de la norma ISO 27001 se permite crear un sistema de gestión de Seguridad de la información como una herramienta indispensable para proteger a las empresas y organizaciones de las amenazas y riesgos contra la información y también, la minimización de las posibles consecuencias

de alguna de las amenazas detectadas.

ISO 27001 es una norma que mantiene la información propia de la empresa, de los clientes y de los proveedores controlada y protegida de cualquier intrusión y posible ciberpirata o ciberatacante.

Brindar seguridad a la información y en las comunicaciones
Para dar una mayor seguridad de datos la Norma ISO 27001, describe el desarrollo de un sistema de gestión de seguridad de la información y define como pueden llegar a abordarse incidentes potenciales dentro de la organización y la definición de métodos de protección a cada incidente presentado.

Por lo tanto, cuando se presenta un caso de pandemia y los empleados inician trabajos desde casa, se deben analizar los tipos de incidentes que pueden llegar a presentar el almacenamiento de información en equipos personales y del envío de información sensible por medio de internet.

Una vez realizado todo el análisis, se podrán seleccionar las mejores herramientas de conexión y dar a conocer los servicios aprobados para compartir datos, para realizar reuniones, para generar copias de seguridad, y/o cualquier otra actividad que requieran los empleados.

Toda esta información deberá ser documentada por medio de políticas y procedimientos y tendrá que darse a conocer para toda la organización y a todos sus empleados de manera organizada.

Datos de contacto:
GRUPO INGERTEC
625 129 170

Nota de prensa publicada en: Madrid

Categorías: Nacional Telecomunicaciones Digital Software Seguridad