Desarrollo de planes de prevención y concienciación en ciberseguridad (Incidentes de ciberseguridad)

Principios generales en materia de ciberseguridad

La ciberseguridad se define como el conjunto de actuaciones orientadas a asegurar, en la medida de lo posible, las redes y sistemas de que constituyen el ciberespacio:

- detectando y enfrentándose a intrusiones,
- detectando, reaccionando y recuperándose de incidentes, y
- preservando la confidencialidad, disponibilidad e integridad de la información.

Normativa de protección del puesto del trabajo

La empresa debe contar con una normativa específica que recoja todas las medidas necesarias para proteger el puesto de trabajo, revisando periódicamente su cumplimiento y modificándola si hubiera cambios que la afecten por ejemplo si se cambian los equipos o los sistemas o se adoptan nuevos servicios.

También se dará a conocer a los empleados otras políticas relativas a los equipos o servicios que utilicen en su desempeño: correo electrónico, almacenamiento, etc.

Plan de formación y concienciación en materia de ciberseguridad

Las personas formamos parte de esta cadena tecnológica como un elemento fundamental e imprescindible. Somos un eslabón que hay que fortalecer, pues se sabe que una cadena es tan fuerte como su eslabón más débil.

Todo el personal de una empresa u organización debe ser consciente de la necesidad de garantizar la seguridad de los sistemas de información, así como ellos mismos son una pieza esencial en el mantenimiento y mejora de la seguridad.

Materiales de formación y concienciación

Es por ello que el Real Decreto 3/2010 de 8 de enero, modificado por el Real Decreto 951/2015, de 23 de octubre, que fija los principios básicos y requisitos mínimos de seguridad, así como las medidas de protección a implantar en los sistemas de la Administración, establece que una de estas medidas será realizar planes de formación y concienciación.

Auditorías internas de cumplimiento en materia de prevención

Las auditorías garantizan el cumplimiento en materia de prevención mediante la revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos.