CONCLUSION

En este módulo de desarrollo y gestión de seguridad en redes se estudiaron los siguientes puntos importantes dentro de la seguridad informática en las organizaciones. Como la seguridad física de los activos de la empresa.

Cuando hablamos de seguridad física nos referimos a todos aquellos mecanismos generalmente de prevención y detección destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un simple teclado hasta una cinta de backup con toda la información que hay en el sistema, pasando por la propia CPU de la máquina. Dependiendo del entorno y los sistemas a proteger esta seguridad será más o menos importante y restrictiva, aunque siempre deberemos tenerla en cuenta. A continuación mencionaremos algunos de los problemas de seguridad física con los que nos podemos enfrentar y las medidas que podemos tomar para evitarlos o al menos minimizar su impacto. El hardware es frecuentemente el elemento más caro de todo sistema informático y por tanto las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización.

Las políticas de seguridad juegan un papel importante dentro de las organizaciones para aquellas que se preocupan de la información que manejan es de suma importancia implementar políticas de seguridad ya que de ellas depende en gran medida que los sistemas estén disponibles y mantener una red limpia sin complicaciones con intrusiones de personas que quieren sacar algún beneficio de la información que maneja la organización. Es frecuente que las personas involucradas con seguridad informática tengan una visión estrecha de lo que significa desarrollar las políticas de seguridad, pues no basta con escribirlas y pretender. Ponerlas en práctica. En ocasiones se incluye la asignación de responsables, se realizan actividades para dar a conocerlas y, quizá, se supervise su cumplimiento; pero esto tampoco basta. Muchas Políticas de seguridad informática fallan ya que se desconoce lo que implica realmente desarrollarlas. Es importante resaltar que una política de seguridad tiene un ciclo de vida completo mientras está vigente. Este ciclo de vida incluye un esfuerzo de investigación, la labor de escribirla, lograr que las directivas de la organización la acepten, conseguir que sea aprobada, lograr que sea diseminada a través de la empresa, concienciar a los usuarios de la importancia de la política, conseguir que la acaten, hacerle seguimiento, garantizar que esté actualizada y, finalmente, suprimirla cuando haya perdido vigencia. Si no se tiene en cuenta este ciclo de vida se corre el riesgo de desarrollar políticas que sean poco tenidas en cuenta, incompletas, redundantes, sin apoyo por parte de los usuarios y las directivas, superfluas o irrelevantes.