Apuntes de Criptografía y Seguridad

Leonardo H. Añez Vladimirovna[1]

Universidad Autónoma Gabriél René Moreno,
Facultad de Ingeniería en Ciencias de la Computación y Telecomunicaciones,
Santa Cruz de la Sierra, Bolivia

1 de diciembre de 2020

[1]Correo Electrónico: toborochi98@outlook.com

Notas del Autor

Estos apuntes fueron realizados durante mis clases en la materia `ELC107 (Criptografía y Seguridad)`, acompañados de referencias de libros, fuentes y código que use a lo largo del curso, en el período `II-2020` en la Facultad de Ingeniería en Ciencias de la Computación y Telecomunicaciones.

Para cualquier cambio, observación y/o sugerencia pueden enviarme un mensaje al siguiente correo:

`toborochi98@outlook.com`

Índice general

Capítulo 1

Conceptos Básicos

1.1. Seguridad Informatica o Seguridad de la Informacion

No es lo mismo seguridad informática que seguridad de la información.

Hoy en día esta demostrado que la información es uno de los activos mas importantes para una empresa u organización y por otra parte, ésta se enfrenta a una variada y cada vez más a diferentes amenazas. Asi mismo, tendremos que entender que nuestra información personal también es importante. Por lo tanto, la conclusión lógica a la que se llega tras un elemental primer análisis de los riesgos a los que se enfrenta dicha información, es que debemos protegerla en sus cuatro estados posibles, esto es cuando dicha información se crea, cuando se transmite, cuando se almacena y cuando se destruye, es decir durante todo su ciclo de vida.

Vamos a pensar un poco. ¿Por qué crees que tiene sentido proteger a la información cuando ésta se destruye? Pon algún ejemplo.

Hasta finales del siglo XX y muy especialmente en entornos no universitarios, era bastante común apreciar una confusión ante la definición y los alcances de la seguridad informática y la seguridad de la información, una situación que hacía suponer a mucha gente que ambos términos eran sinónimos y que, por tanto, significaban lo mismo. Como a fecha de hoy se sigue observando dicha confusión y dado que la diferencia entre ambas es ya muy marcada, resulta recomendable dedicar esta primera lección para aclarar conceptos, observar similitudes y resaltar sus diferencias. No obstante, ante la duda de usar un término u otro, tal como veremos en esta lección, hoy en día lo más correcto sería referirnos a todo esto como seguridad de la información, al ser este último término más amplio que el de seguridad informática.

Seguridad informática

Cuando nos referimos a seguridad informática, estamos centrando nuestra atención sólo en los aspectos de seguridad que inciden o tienen que ver directamente con la informática; es decir, en los medios informáticos en los que se genera, gestiona, almacena o destruye esta información, pero sin profundizar en aspectos sistémicos de la gestión de esa seguridad. Ateniéndonos entonces en primera instancia a las temáticas propias de la seguridad informática, entendida ésta según lo indicado en el párrafo anterior, que por lo demás es como se conocía a esta especialidad en sus inicios desde el nacimiento de la computación, podríamos representarla en 7 grandes apartados, cada uno de ellos con entidad suficiente como para convertirse en una especialidad tecnológica:

1. Protección y seguridad de los datos
2. Criptografía
3. Seguridad y fortificación de redes
4. Seguridad en aplicaciones informáticas,programas y bases de datos.
5. Gestión de seguridad en equipos y sistemas informáticos
6. Informática forense
7. Ciberdelito, ciberseguridad

Seguridad de la información

Cuando además de lo anterior tenemos en cuenta aquellos aspectos sistémicos de la gestión de la seguridad, como podrían ser por ejemplo en una empresa u organización las políticas y planes de seguridad con su respectivo análisis y gestión del riesgo, la continuidad del negocio, la adecuación al entorno legal y a las normativas internacionales, entonces es más propio hablar de seguridad de la información. Esto es debido a que en la actualidad existen otras temáticas muy importantes que están relacionadas con la seguridad de la información y la protección de los datos pero que, a diferencia de los apartados vistos anteriormente, su entorno no está físicamente tan cerca de los equipos informáticos y de las redes, sino de la gestión, de la gerencia y del buen gobierno de la empresa. Entre estos otros temas más propios de un entorno empresarial, se pueden contemplar también 7 grandes apartados, a saber:

1. Gestión de la seguridad de la información
2. Asesoría y auditoría de la seguridad
3. Análisis y gestión de riesgos
4. Continuidad de negocio
5. Buen gobierno
6. Comercio electrónico
7. Legislación relacionada con seguridad