1.1.- PILARES DE SEGURIDAD DE SISTEMAS

Los datos son valores, números, medidas, textos, documentos en bruto, la información es el valor de esos datos, es lo que aporta conocimiento. Los manuales de procedimientos, los datos de los empleados, de los proveedores y clientes de la empresa, la base de datos de facturación son datos estructurados de tal forma que se convierten en información, que aportan valor como empresa u organización.

Los pilares de la seguridad de sistemas se fundamentan en esa necesidad que todos tienen de obtener la información, de su importancia, integridad y disponibilidad de la información para sacarle el máximo rendimiento con el mínimo riesgo. La Figura 1 muestra los principales pilares de la seguridad de la información.

Figura 1. Pilares de la seguridad**.**

Según la Figura 1, la seguridad está fundamentada por 3 pilares, pero puede haber más que puedan fundamentar a la seguridad, en este caso, si alguno de los lados es débil se perderá seguridad o usabilidad, si falta alguno de los lados la organización queda expuesta a ataques, para esto se debe conocer en detalle cuál es la función de cada lado en el gráfico.

Ahora que se compre la importancia de la información se puede deducir que si aquella, que es vital para la organización cayera en manos inapropiadas puede perder su valor, se perderá intimidad o capacidad de maniobra y además la reputación puede verse dañada sin contar con que la información puede ser accedida por cibercriminales y cualquier otra potencial fuente de riesgos para un determinado proyecto.

CONFIDENCIALIDAD: La confidencialidad consiste en asegurar que sólo el personal autorizado accede a la información que le corresponde, de este modo cada sistema automático o individuo solo podrá usar los recursos que necesita para ejercer sus tareas, para garantizar la confidencialidad se recurre principalmente a tres recursos:

- **Autenticación de usuarios**: Sirve para identificar qué quién accede a la información es quien dice ser.

- **Gestión de privilegios**: Para los usuarios que acceden a un sistema puedan operar sólo con la información para la que se les ha autorizada y sólo en la forma que se les autorice, por ejemplo, gestionando permisos de lectura o escritura en función del usuario.

- **Cifrado de información**: Según Costas Santos (2011), el cifrado también denominado encriptación, evita que ésta sea accesible a quién no está autorizado, para ello se transforma la información de forma inteligible a una no legible y es aplicable tanto a la información que esté autorizado para ello como para la que no lo está, sólo mediante un sistema de contraseñas puede extraerse la información de forma inteligible y es aplicable tanto a la información que está siendo transmitida como a la almacenada.

Los principios de confidencialidad no solo deben aplicarse para proteger la información sino todos aquellos datos e información de los que sea responsables. La información puede tener carácter confidencial no solo por ser de alto valor para la organización, sino por ejemplo porque puede estar amparada por legislación de protección de datos de carácter personal, un ejemplo de violación de la confidencialidad son las filtraciones

sufridas por entidades bancarias, grandes empresas y gobiernos para exponer públicamente algunas de sus actividades.

LA INTEGRIDAD: Es el segundo pilar de la seguridad, consiste en asegurarse de que la información no se pierde ni se ve comprometida voluntaria e involuntariamente, el hecho de trabajar con información errónea puede ser tan nocivo para las actividades como perder la información, de hecho, si la manipulación de la información es lo suficientemente sutil puede causar que se arrastre una cadena de errores acumulativos y que sucesivamente se tome decisiones equivocadas. Para garantizar la integridad de la información se debe considerar lo siguiente:

1. **Monitorear el tráfico de red** para descubrir posibles intrusiones.

2. **Auditar los sistemas** para implementar políticas de auditorías que registre quien hace que, cuando y con qué información.

3. **Implementar sistemas de control de cambios**, algo tan sencillo como por ejemplo comprobar los resúmenes de los archivos de información almacenados en sistema para comprobar si cambian o no.

4. Como otro recurso se tiene las **copias de seguridad**, que en caso de no conseguir impedir que se manipule o pierda la información permitan recuperarla en su estado anterior.

DISPONIBILIDAD: Para poder considerar que se dispone de una seguridad mínima en lo que a la información respecta, se tiene a la disponibilidad, de nada sirve que solo el usuario acceda a la información y que sea incorruptible, si el acceso a la misma es tedioso o imposible, la información para resultar útil y valiosa debe estar disponible para quien la necesita, se debe implementar las medidas necesarias para que tanto la información como los servicios estén disponibles, por ejemplo un ataque distribuido de denegación de servicio o DDoS puede dejar inutilizada una tienda online impidiendo que los clientes accedan a la misma y puedan comprar. Ogro ejemplo de perdida de disponibilidad sería que la dirección de correo electrónico sea utilizada para lanzar campañas de spam y en consecuencia añadida a listas negras, impidiendo que ninguno

de los destinarios de los emails legítimos los reciba. Para este propósito se implementan políticas de control como:

- El acuerdo de nivel de servicio o (SLA).
- Balanceadores de carga de tráfico para minimizar el impacto de DDoS.
- Copias de seguridad para restauración de información perdida.
- Disponer de recursos alternativos a los primarios.

La información y sistemas son seguros si sólo accede a la información y recursos quién debe, sí se puede detectar y recuperar de manipulaciones voluntarias o accidentales de la información y si se puede garantizar un nivel de servicio y acceso a la información aceptable según las necesidades.

Carpentier (2016), indica que el uso de sistemas de información implica establecer normas y procedimientos aplicados al uso y sistemas de información ante posibles amenazas como:

- Elaborar varias normas y procedimientos.
- Definición de acciones que deben emprender las personas.
- Definición del perímetro que se va a afectar.

EVALUACIÓN DE RIESGOS, AMENAZAS Y VULNERABILIDADES

Cuando se plantea mejorar la seguridad de una empresa se debe tener en cuenta varios factores que se muestra a continuación:

- Recursos
- Amenazas
- Vulnerabilidades
- Riesgos

Se entiende a los **recursos** como los bienes tangibles e intangibles con los que se cuenta para realizar las tareas, la información de que se dispone es un bien intangible, ya sean las bases de datos de clientes, proveedores, los manuales de producción, las investigaciones y las patentes. Por otro lado, se tiene a los bienes tangibles, qué son los recursos físicos de que se dispone en la empresa, servidores, equipos de red, computadoras, teléfonos inteligentes, vehículos, bienes inmuebles, etc., la Figura 2 muestra un ejemplo de bienes tangibles e intangibles.

Figura 2. Ejemplo de bienes tangibles e intangibles**. Fuente:** https://ciberconta.unizar.es/ifinanzas/10-intangibles.htm

El **riesgo** es la probabilidad de que algo negativo suceda dañando los recursos tangibles o intangibles y por tanto impidiendo desarrollar la labor profesional.

Las **amenazas** son esos sucesos que pueden dañar los procedimientos o recursos, mientras que las **vulnerabilidades** son los fallos de los sistemas de seguridad o en los propios que el usuario utiliza para desarrollar las actividades que permitirían que una amenaza tuviese éxito a la hora de generar un problema. El principal trabajo de un responsable de la seguridad es la evaluación de los riesgos identificando las vulnerabilidades, amenazas y en base a esta información evaluar los riesgos a los que están sujetos las actividades y recursos.