



INICIO GRABACIÓN



SANJOSÉ
FUNDACIÓN DE EDUCACIÓN SUPERIOR



FUNDAMENTOS DE LA CIBERSEGURIDAD

se analizará los conceptos relacionados a la ciberseguridad, sobre las amenazas, riesgos y vulnerabilidades que hay en una organización, se tratará también sobre las diferentes superficies de ataques que pueden existir para que un cibercriminal pueda lanzar su ataque, se analizará en que consiste la ingeniería social y la ley de mínimos privilegios.




Los tres pilares de la seguridad



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 compañía.

Los pilares de la seguridad de la información 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 3 muestra los principales pilares de la seguridad de la información.

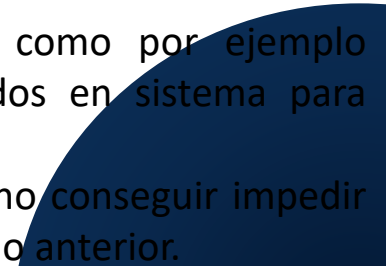




Confidencialidad: La confidencialidad consiste en asegurar que sólo el personal autorizado accede a la información que le corresponde, de este modo cada sistema automático o individuo solo podrá usar los recursos que necesita para ejercer sus tareas, para garantizar la confidencialidad se recurre principalmente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

- Autenticación de usuarios
- Gestión de privilegios
- Cifrado de información

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.

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.

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.



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.





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.



Tipos de amenazas



Existen amenazas difícilmente controlables como las naturales como los desastres o errores humanos, pero que deben ser tenidas en cuenta a la hora de calcular riesgos, una persona podría borrar accidentalmente información de un servidor o podría enviar un correo electrónico con información confidencial a un destinatario erróneo, del mismo modo el Hardware de los recursos informáticos de la empresa puede verse dañado por el uso, por inundaciones, fallas eléctricas, etc.

Vulnerabilidades

Las vulnerabilidades son por lo general fallos de diseño de procedimientos o de recursos, las vulnerabilidades existen no se fabrican, una vulnerabilidad es cualquier fallo de diseño que permite que una amenaza pueda afectar a un recurso. Si se habla de recursos informáticos se suele decir que una vulnerabilidad es un fallo de diseño de un sistema, un sistema no actualizado o un sistema mal Configurado que permite que un agente externo, acceda sin permisos apropiados al recurso o información que dicho sistema gestiona, en función del tipo de recurso al que estemos orientados existen distintas fuentes de información dónde se puede buscar vulnerabilidades aplicables a los sistemas con que se cuenta.

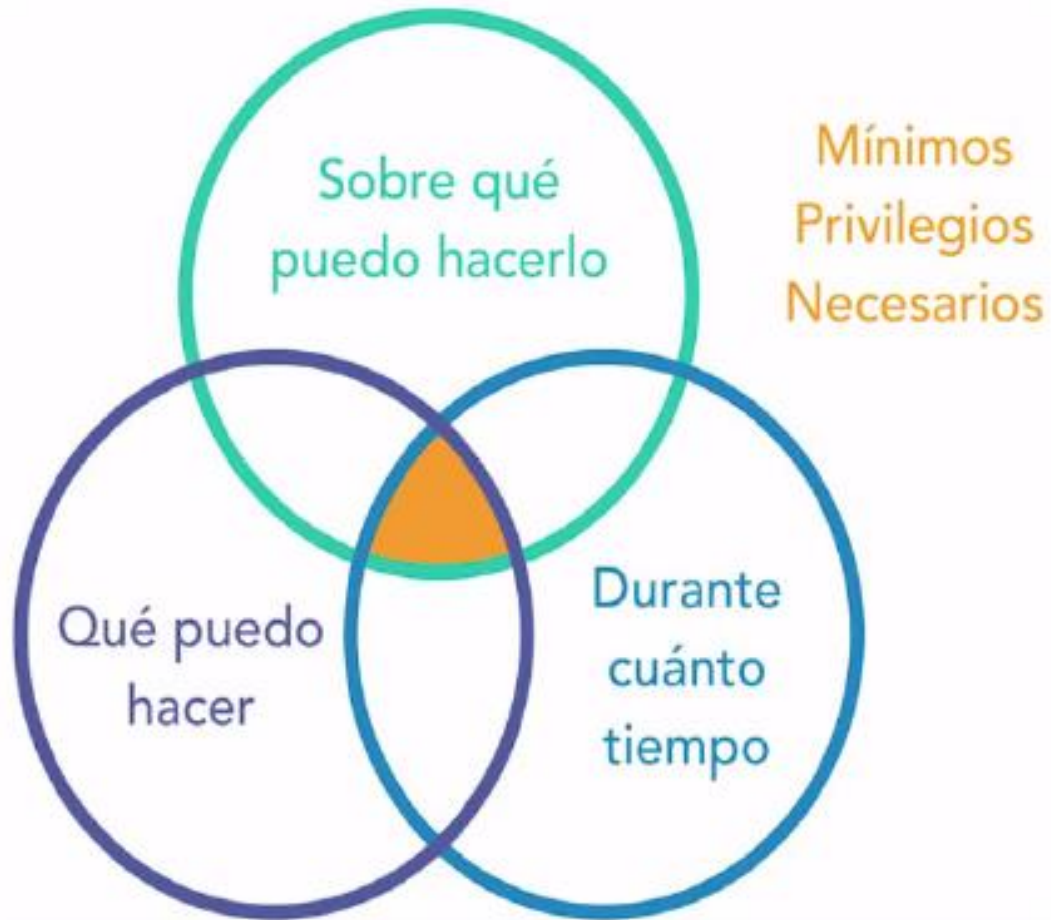
Ley de mínimos privilegios



Al implementar cualquier sistema organizativo, de reparto de tareas y responsabilidades se debe tener claro que no todo el mundo tiene porque acceder a todos los recursos de la organización, ni tiene que hacerlo de forma permanente. Cada individuo y cada herramienta debe acceder solo a aquello imprescindible para el desempeño de sus funciones, sabiendo a lo que se puede acceder y a lo que no, hay que decidir qué se puede hacer con la información o recursos a los que se tiene acceso, a esto se le denomina **privilegios y permisos**.



Ley de mínimos privilegios






Ingeniería social



La ingeniería social es cualquier acto que induce a una persona a realizar una acción que puede, o no, ser en su mejor interés.

Una de las formas más habituales de uso de la ingeniería social para atacar infraestructuras informáticas es la obtención de información personal de la plantilla de una organización, consciente que dicha información permita descubrir contraseñas y acceso a recursos restringidos. También se usa la ingeniería social para generar campañas genéricas de email fraudulentos conocidas como **Phishing**, destinadas a distribuir por ejemplo malware.

Actualmente la ingeniería social es el principal método de distribución de ransomware, un malware que cifra los archivos y pide un rescate económico. El Phishing funciona porque el email parece auténtico, suplanta la identidad corporativa de una empresa reconocible, es muy común suplantar a compañías eléctricas, proveedores de servicios telefónicos, el caso del espía Phishing es una variación del Phishing que, en lugar de distribuirse masivamente, emplea email redactados y diseñados para engañar específicamente a una persona.





Software

Está compuesto de aplicaciones, servicios, ejecutables, páginas web y otros servicios como NFTP, TELNET y otros similares. Las vulnerabilidades en el software son fallas en la programación o compilación de los programas que ejecutan las computadoras a servidores, los ataques a estas vulnerabilidades pueden derivar en un mal funcionamiento del software, acceso a información restringida, fallos de sistema, etc. Para reducir esta superficie de ataque, hay que reducir al mínimo el software instalado en las computadoras y servidores, mantener actualizado el software y aplicar todos los parches de seguridad publicados por los desarrolladores.

ConFigurar el software con la ley de los mínimos privilegios en mente, no utilizar software pirata o de fuentes no confiables y explorar recurrentemente las bases de datos públicas de vulnerabilidades en busca de aquellas que puedan afectar al software.


Hardware

Estadísticamente hablando el hardware es la segunda superficie de ataque a considerar, lo común es que, para atacar a un dispositivo hardware, el atacante necesita tener acceso físico al dispositivo. En este caso es fácil analizar que las amenazas naturales como fallos por envejecimiento de equipos o desastres como robos, incendios o inundaciones, afecta específicamente a esta superficie de ataque.

Los ataques a hardware también pueden producirse a través de la red o afectando al medio físico de transmisión, por ejemplo, los perturbadores de señal pueden interrumpir las comunicaciones de distinto tipo de tecnología inalámbrica mediante la generación de ruido radioeléctrico en la frecuencia y forma correcta. Este tipo de ataques podría anular sistemas de comunicaciones de los que dependen alarmas, sensores o cualquier otro tipo de comunicaciones, ya sean entre dispositivos o personas.



Recursos humanos



Por último, esta es la última superficie de ataque correspondiente a los recursos humanos, que pueden actuar contra los intereses de la organización por descontento, error, engaño o coacción. Además de implementar y exigir el cumplimiento de protocolos de actuación, es aconsejable implementar sistemas de registro y auditoría para verificar quién hace qué y cuándo, de este modo al evitar el anonimato se minimiza la probabilidad de éxito de una amenaza de carácter humano, además se debe invertir esfuerzo y recursos en educar y concienciar a los usuarios de nuestros recursos e infraestructuras para que se impliquen a la hora mantener un alto nivel de seguridad.



FUNDACIÓN DE EDUCACIÓN SUPERIOR

SAN JOSÉ

INSTITUCIÓN TECNOLÓGICA

FIN DE
GRABACIÓN