ANÁLISIS DE RIESGO

En la actualidad, las tecnologías de la información (TI) juegan un rol fundamental en los diversos procesos de negocio, por lo que deben verse como un activo estratégico y no solo como un activo operativo.

Para garantizar el uso eficiente de los recursos informáticos y convertir las TI en un activo estratégico, se deben implementar buenas prácticas en la gestión de los servicios de TI. Hay que considerar que el uso de las TI implica riesgos que deben ser gestionados mediante diversas técnicas, marcos de trabajo y normas internacionales existentes en seguridad informática que garanticen que las TI sean un aliado en la consecución de los objetivos de negocio. En caso de no gestionar debidamente los riesgos generados por el uso de las TI, estas se convertirán más en un problema que en una solución para la organización.

ANÁLISIS Y GESTIÓN DE RIESGOS

Antes de implementar un sistema de seguridad de la información, se debe tener claridad respecto a qué se debe proteger y contra qué se va a proteger, para posteriormente determinar cómo se va a proteger en función de las expectativas y los objetivos organizacionales. Esto surge de un análisis de riesgos.

Por medio del análisis de riesgos, una organización conoce a qué está expuesta, le permite identificar los riesgos que le podrían impedir lograr sus objetivos de negocio, determinando su magnitud e identificando las áreas que requieren medidas de salvaguarda o controles en función del riesgo detectado.

El análisis de riesgos permite determinar cómo es, cuánto vale y qué tan protegido se encuentra el sistema. En coordinación con los objetivos, estrategias y políticas de la organización, las actividades de tratamiento de los riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la dirección.

La implantación de las medidas de seguridad requiere una organización gestionada y la participación consciente de todo el personal que trabaja con el sistema de información. Este personal es el responsable de la operación diaria, de la reacción ante incidencias y del monitoreo en general del sistema, para determinar si satisface con eficacia y eficiencia los objetivos propuestos.

Este esquema de trabajo debe ser repetitivo, pues los sistemas de información rara vez son inmutables; más bien se encuentran sometidos a evolución continua tanto propia (nuevos activos) como del entorno (nuevas amenazas), lo que exige una revisión periódica en la que se aprende de la experiencia y se adapta al nuevo contexto.

SEGURIDAD PERIMETRAL Y DE PUNTO FINAL

El perímetro de una red de computadores es la frontera virtual existente entre la red interna de la organización y otras redes donde la más habitual es Internet. De todos los incidentes de seguridad que pueden presentarse, la mayoría provienen del perímetro puesto, que es la frontera entre una red "segura" (la de la organización) y una red no segura (Internet), en la cual se mueven muchos agentes maliciosos que tienen como objetivo ingresar de forma no autorizada en las organizaciones, principalmente con fines económicos.

Debemos dar seguridad a nuestro perímetro, para lo que podemos utilizar diversas soluciones como son: Firewalls, IDS, IPS, VPN, entre otros.

Por otro lado, la seguridad de punto final se refiere a aquellas medidas que se toman para asegurar los equipos de cómputo frente a las diversas amenazas que puedan surgir. A diferencia de la seguridad perimetral que protege el perímetro de la red, la de punto final se encargada de dar seguridad dentro de ese perímetro, es decir dentro de la red.

SI un funcionario de la organización introduce una memoria USB que está infectada con algún agente malicioso, los equipos de seguridad perimetral no tendrán cómo detectar esa amenaza, ya que solo se encargan de vigilar el perímetro. Es entonces cuando entran en juego las medidas de protección de punto final como los antivirus, antimalware, aplicaciones firewall, etc.

SEGURIDAD INFORMÁTICA

El uso de Tecnologías de Información y Comunicación (TIC) puede dar lugar a ciertos riesgos que deben gestionarse con medidas de seguridad.

Los sistemas informáticos están expuestos a amenazas de todo tipo. Primero, se deben identificar para evaluarlas y decidir qué medidas de seguridad se adoptarán para mitigar el riesgo que suponen. Decidir si vale la pena implantar una contramedida o si es mejor aceptar el riesgo tal cual. Eliminar el riesgo por completo es imposible, pero se puede reducir a niveles aceptables que permitan convivir con él.

La seguridad de la información requiere un enfoque holístico, que implique la participación coordinada de tecnología, personas y operaciones. Su objetivo no es conseguir sistemas 100% seguros, sino sistemas tan seguros como sea necesario para proteger los activos con un nivel que se corresponda con la expectativas.

central 2511-5000
ci5000@ucr.ac.cr
www.facebook.com/ciucr/
twitter.com/ciucr
UNIVERSIDAD DE COSTA RICA
CI
Centro de **Informática**