Presentación Corporativa

Servicios de Ciberseguridad y seguridad de la información

Fco. Javier Marqués Pons
Ingeniero en Sistemas de Telecomunicación y Máster en Ingeniería Telemática
Colegiado COGITT Nº 9724 y Perito Judicial Tecnológico CNIPJ

TELingeNET Informática e Ingeniería
forenseTIC Peritajes y Ciberseguridad

La **ciberseguridad** de acuerdo con ISACA (Asociación de Auditoria y Control de Sistemas de información) se define como: "**Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados**".

Es decir: define todos los conceptos que rigen la seguridad a través de Internet y las redes de datos**,** como pueden ser los datos personales, información bancaria, claves, compras online…

La cantidad de información que circula por la Red es muy grande, y los riegos se hacen patentes cada día con mayor riesgos para la persona, pero también para las empresas, las instituciones e incluso los países.

El entorno en el que nos movemos diariamente por las redes de datos son cada día más grandes, y precisamente la ciberseguridad debe garantizar la seguridad de todos nuestros "movimientos" en la Internet y las redes de datos.

La Ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización. Dichas propiedades de seguridad incluyen las siguientes tres dimensiones: **disponibilidad, integridad, confidencialidad.**

Esperar a que las **ciberamenazas** existentes se materialicen no es una opción, ya que la pérdida o revelación de información crítica del negocio podría traer consigo graves consecuencias para la organización.

Seis de cada siete empresas son afectadas y éstas desconocen inclusive que han sido víctimas. Muchos de estos ataques en los próximos años cambiarán sus técnicas de infección y procesos de identificación con la finalidad de volverse mayormente evasivas.

Muchas de las herramientas conocidas hoy en día tienen como objetivo principal el prevenir y mitigar los delitos telemáticos protegiendo siempre la integridad de los datos y la reputación de las empresas. **Las empresas deben tomar más conciencia de que estos crímenes están latentes y no esperar a que les suceda, y desde forenseTIC le ayudaremos a esto.**

El Departamento de **Ciberseguridad** de **forenseTIC Peritajes y Ciberseguridad** ofrece servicios que le permitirán conocer y controlar las ciberamenazas a las que están expuestos sus sistemas y datos: Análisis de Vulnerabilidades, Auditoría de Seguridad de Sistemas y WIFI, Hacking ético, etc…

Algunas explicaciones de lo que hacemos para garantizar la seguridad en forenseTIC:

Seguridad de la información

La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información, si alguna de estas características falla no estamos ante nada seguro. Es preciso anotar, además, que la seguridad no es ningún hito, es más bien un proceso continuo que hay que gestionar conociendo siempre las vulnerabilidades y las amenazas que se ciñen sobre cualquier información, teniendo siempre en cuenta las causas de riesgo y la probabilidad de que ocurran, así como el impacto que puede tener. **Una vez conocidos todos estos puntos, y nunca antes, deberán tomarse las medidas de seguridad oportunas.**

Confidencialidad

La confidencialidad es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito a ser transmitida desde el comprador al comerciante y el comerciante de a una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos. Si una parte no autorizada obtiene el número de la tarjeta en modo alguno, se ha producido una violación de la confidencialidad.

La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla, cuando se publica información privada, cuando un laptop con información sensible sobre una empresa es robado, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad.

Integridad

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. *Grosso modo*, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

La integridad también es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada, para salvaguardar la precisión y completitud de los recursos.

La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra datos importantes que son parte de la información.

La integridad garantiza que los datos permanezcan inalterados excepto cuando sean modificados por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital es uno de los pilares fundamentales de la seguridad de la información.

Disponibilidad

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Grosso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La alta disponibilidad sistemas objetivo debe estar disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

Garantizar la disponibilidad implica también la prevención de ataque de denegación de servicio. Para poder manejar con mayor facilidad la seguridad de la información, las empresas o

negocios se pueden ayudar con un sistema de gestión que permita conocer, administrar y minimizar los posibles riesgos que atenten contra la seguridad de la información del negocio.

La disponibilidad además de ser importante en el proceso de seguridad de la información, es además variada en el sentido de que existen varios mecanismos para cumplir con los niveles de servicio que se requiera. Tales mecanismos se implementan en infraestructura tecnológica, servidores de correo electrónico, de bases de datos, de web etc, mediante el uso de clusters o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, etc. **La gama de posibilidades dependerá de lo que queremos proteger y el nivel de servicio que se quiera proporcionar, y esto se estudia por los profesionales de forenseTIC para darle el servicio que el cliente nos pida.**

Planificación de la seguridad

Hoy en día la rápida evolución del entorno técnico requiere que las organizaciones adopten un conjunto mínimo de controles de seguridad para proteger su información y sistemas de información. El propósito del plan de seguridad del sistema que ofrecemos en forenseTIC es proporcionar una visión general de los requisitos de seguridad del sistema y se describen los controles en el lugar o los previstos para cumplir esos requisitos.

El plan de seguridad del sistema también delinea las responsabilidades y el comportamiento esperado de todos los individuos que acceden al sistema. Debe reflejar las aportaciones de distintos gestores con responsabilidades sobre el sistema, incluidos los propietarios de la información, el propietario de la red, y el alto funcionario de la agencia de información de seguridad (SAISO).

Los administradores de programas, los propietarios del sistema, y personal de seguridad en la organización debe entender el sistema de seguridad en el proceso de planificación. Los responsables de la ejecución y gestión de sistemas de información deben participar en el tratamiento de los controles de seguridad que deben aplicarse a sus sistemas.

Creación de un plan de respuesta a incidentes

Es importante formular un plan de respuestas a incidentes, soportarlo a lo largo de la organización y probarlo regularmente. Un buen plan de respuestas a incidentes puede no sólo minimizar los efectos de una violación sino también, reducir la publicidad negativa.

Desde la perspectiva del equipo de seguridad, no importa si ocurre una violación o abertura (pues tales eventos son una parte eventual de cuando se hacen negocios usando un método de poca confianza como lo es Internet), sino más bien cuándo ocurre. El aspecto positivo de entender la inevitabilidad de una violación a los sistemas (cualquier sistema donde se procese información confidencial, no está limitado a servicios informáticos) es que permite al equipo de seguridad desarrollar un curso de acciones para minimizar los daños potenciales. Combinando un curso de acciones con la experiencia le permite al equipo responder a condiciones adversas de una manera formal y oportuna.

El plan de respuesta a incidentes puede ser dividido en cuatro fases:

- **Acción inmediata para detener o minimizar el incidente**
- **Investigación del incidente**
- **Restauración de los recursos afectados**
- **Reporte del incidente a los canales apropiados**

Una respuesta a incidentes debe ser decisiva y ejecutarse rápidamente. Debido a que hay muy poco espacio para errores, es crítico que se efectúen prácticas de emergencias y se midan los tiempos de respuesta. De esta forma, es posible desarrollar una metodología que fomenta la velocidad y la precisión, minimizando el impacto de la indisponibilidad de los recursos y el daño potencial causado por el sistema en peligro.

Un plan de respuesta a incidentes tiene un número de requerimientos, incluyendo:

- **Un equipo de expertos locales (un Equipo de respuesta a emergencias de computación)**
- **Una estrategia legal revisada y aprobada**
- **Soporte financiero de la compañía**

- **Soporte ejecutivo de la gerencia superior**
- **Un plan de acción factible y probado**
- **Recursos físicos, tal como almacenamiento redundante, sistemas en stand by y servicios de respaldo**

Planes de acción

Una vez creado un plan de acción, este debe ser aceptado e implementado activamente. Cualquier aspecto del plan que sea cuestionado durante la implementación activa lo más seguro es que resulte en un tiempo de respuesta pobre y tiempo fuera de servicio en el evento de una violación. Aquí es donde los ejercicios prácticos son invalorables. La implementación del plan debería ser acordada entre todas las partes relacionadas y ejecutada con seguridad, a menos que se llame la atención con respecto a algo antes de que el plan sea colocado en producción.

La respuesta a incidentes debe ir acompañada con recolección de información siempre que esto sea posible. Los procesos en ejecución, conexiones de red, archivos, directorios y mucho más deberían ser auditados activamente en tiempo real. Puede ser muy útil tener una toma instantánea de los recursos de producción al hacer un seguimiento de servicios o procesos maliciosos. Los miembros de CERT y los expertos internos serán recursos excelentes para seguir tales anomalías en un sistema.

El manejo de riesgos

Dentro de la seguridad en la información se lleva a cabo la clasificación de las alternativas para manejar los posibles riegos que un activo o bien puede tener dentro de los procesos de organización. Esta clasificación lleva el nombre de manejo de riesgos. El manejo de riesgos, conlleva una estructura bien definida, con un control adecuado y su manejo, habiéndolos identificado, priorizados y analizados, a través de acciones factibles y efectivas. Para ello se cuenta con las siguientes técnicas de manejo del riesgo:

- **Evitar.** El riesgo es evitado cuando la organización rechaza aceptarlo, es decir, no se permite ningún tipo de exposición. Esto se logra simplemente con no comprometerse a realizar la acción que origine el riesgo. Esta técnica tiene más desventajas que ventajas, ya que la empresa podría abstenerse de aprovechar muchas oportunidades. Ejemplo:

  No instalar empresas en zonas sísmicas

- **Reducir.** Cuando el riesgo no puede evitarse por tener varias dificultades de tipo operacional, la alternativa puede ser su reducción hasta el nivel más bajo posible. Esta opción es la más

económica y sencilla. Se consigue optimizando los procedimientos, la implementación de controles y su monitoreo constante. Ejemplo:

No fumar en ciertas áreas, instalaciones eléctricas anti flama, planes de contingencia.

- **Retener, Asumir o Aceptar el riesgo**. Es uno de los métodos más comunes del manejo de riesgos, es la decisión de aceptar las consecuencias de la ocurrencia del evento. Puede ser voluntaria o involuntaria, la voluntaria se caracteriza por el reconocimiento de la existencia del riesgo y el acuerdo de asumir las perdidas involucradas, esta decisión se da por falta de alternativas. La retención involuntaria se da cuando el riesgo es retenido inconscientemente. Ejemplo de asumir el riesgo:

  Con recursos propios se financian las pérdidas.

- **Transferir.** Es buscar un respaldo y compartir el riesgo con otros controles o entidades. Esta técnica se usa ya sea para eliminar un riesgo de un lugar y transferirlo a otro, o para minimizar el mismo, compartiéndolo con otras entidades. Ejemplo:

  Transferir los costos a la compañía aseguradora

Medios de transmisión de ataques a los sistemas

El mejor en soluciones de su clase permite una respuesta rápida a las amenazas emergentes, tales como:

- Malware y spam propagado por e-mail.
- La propagación de malware y botnets
- Los ataques de phishing alojados en sitios web.
- Los ataques contra el aumento de lenguaje de marcado extensible (XML) de tráfico, arquitectura orientada a servicios (SOA) y servicios web.

Estas soluciones ofrecen un camino a la migración y la integración. Como las amenazas emergentes, cada vez más generalizada, estos productos se vuelven más integrados en un enfoque de sistemas.

Un enfoque de sistemas de configuración, la política, y el seguimiento se reúne cumplimiento de las normativas en curso y permite a los sistemas rentables de gestión. **El enfoque de sistemas de gestión de la seguridad, dispone:**

- **Configuración de la política común de todos los productos**
- **Amenaza la inteligencia y la colaboración de eventos**
- **Reducción de la complejidad de configuración**
- **Análisis de riesgos eficaces y operativos de control**

Tecnologías que utilizamos en forenseTIC

Las principales tecnologías referentes a la seguridad de la información en telemática son:

- Cortafuegos
- Administración de cuentas de usuarios
- Detección y prevención de intrusos
- Antivirus
- Infraestructura de llave publica
- Capas de Socket Segura (SSL)
- Conexión única "Single Sign on- SSO"
- Biométria
- Cifrado
- Cumplimiento de privacidad
- Acceso remoto
- Firma digital
- Intercambio electrónico de Datos "EDI" y Transferencia Electrónica de Fondos "EFT"
- Redes Virtuales Privadas "VPNs"
- Transferencia Electrónica Segura "SET"
- Informática Forense
- Recuperación de datos
- Tecnologías de monitoreo