Categorización funcional de los diferentes tipos de controles de seguridad y su aplicabilidad en la estrategia de protección corporativa

Con el objetivo de establecer una estrategia para la gestión de los potenciales riesgos en términos de confidencialidad, integridad y disponibilidad en un entorno de tecnología de la información (TI) –identificados mediante la ejecución metodológica de un análisis de riesgos– es necesario proceder con el despliegue de una serie de medidas coordinadas a lo largo del tiempo. Dichas medidas se conocen como "controles de seguridad" y están orientadas al mantenimiento del riesgo dentro de unos umbrales aceptables para la organización. En este artículo se describirán las diferentes categorías de controles de seguridad, su aplicabilidad y la asignación de responsabilidades para su gestión.

David E. Acosta Rodríguez

A pesar de que es imposible que estos controles ofrezcan unos niveles perfectos de efectividad y eficiencia, la clave para la optimización de su desempeño está en conocer los diferentes tipos disponibles para poder implementarlos dependiendo del activo a proteger, el intervalo de tiempo en el que actuará y su integración con otros controles en una maniobra conjunta y global. Precisamente, muchos marcos de trabajo, buenas prácticas y estándares de seguridad de la información (tales como ISO/IEC 27002[1], los controles de seguridad del CIS[2] y el marco de ciberseguridad del NIST[3], entre otros) definen una serie de acciones para permitir la alineación metodológica de estos controles dentro de la infraestructura de la organización.

En este artículo se describirán las diferentes categorías de controles de seguridad, su aplicabilidad y la asignación de responsabilidades para su gestión con base en el diagrama (ver **Figura 1**).

Categorización de controles con base en su aplicabilidad

En términos generales, los controles de seguridad se pueden dividir en tres grandes grupos dependiendo de su ámbito de aplicabilidad:

– **Controles de seguridad físicos u operacionales**: Son aquellos tipos de controles tangibles orientados a la protección del entorno y de los recursos físicos de la organización.

Ejemplos:
· Puertas
· Cerraduras
· Ventanas

– **Controles de seguridad lógicos o técnicos**: Son aquellos controles basados en una combinación de hardware y software.

Ejemplos:
· Criptografía
· Antimalware
· Cortafuegos ("firewalls")

– **Controles de seguridad administrativos o de gestión**: Son aquellos controles procedimentales, administrativos y/o documentales que establecen las reglas a seguir para la protección del entorno.

Ejemplos:
· Política de seguridad
· Gestión de privilegios
· Controles de contratación de personal.

Categorización de controles con base en su comportamiento

De acuerdo con los principios estratégicos militares, cualquier confrontación cuenta con un agente que actúa como ofensivo y otro que actúa como defensivo, pudiendo cambiar sus papeles a lo largo del desarrollo del conflicto. En una actitud ofensiva siempre se toma la iniciativa y se desarrollan acciones orientadas a atacar al otro, mientras que en la actitud defensiva se renuncia a la iniciativa y se espera al ataque para contenerlo y repelerlo[4]. Si se aplican los mismos criterios en el ámbito de seguridad de la información, se pueden establecer dos categorías principales de controles de seguridad dependiendo de su comportamiento: **Controles defensivos y controles ofensivos.**

La optimización de los controles defensivos se basa en la existencia de su contraparte: los controles ofensivos. Mediante esta interacción, la organización podrá monitorizar la efectividad y eficiencia de su estrategia, obtener evidencias e indicadores claves para la mejora continua y alinear los niveles de seguridad con base en las necesidades del negocio.

La coordinación entre los controles defensivos y ofensivos de la organización y la aplicación de acciones de mejora continua con base en los resultados de sus

[1] ISO/IEC 27002: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534

[2] Center for Internet Security – CIS Controls: https://www.cisecurity.org/controls/

[3] Guía rápida para entender el marco de trabajo de ciberseguridad del NIST: https://www.deacosta.com/guia-rapida-para-entender-el-marco-de-trabajo-de-ciberseguridad-del-nist/

[4] ISACA JOnline - "Posición Estratégica Defensiva" en el Campo de Seguridad de la Información: http://www.isaca.org/Journal/archives/2013/Volume-6/Pages/JOnline-Defensive-Strategic-Posture-in-the-Field-of-Information-Security-Spanish.aspx

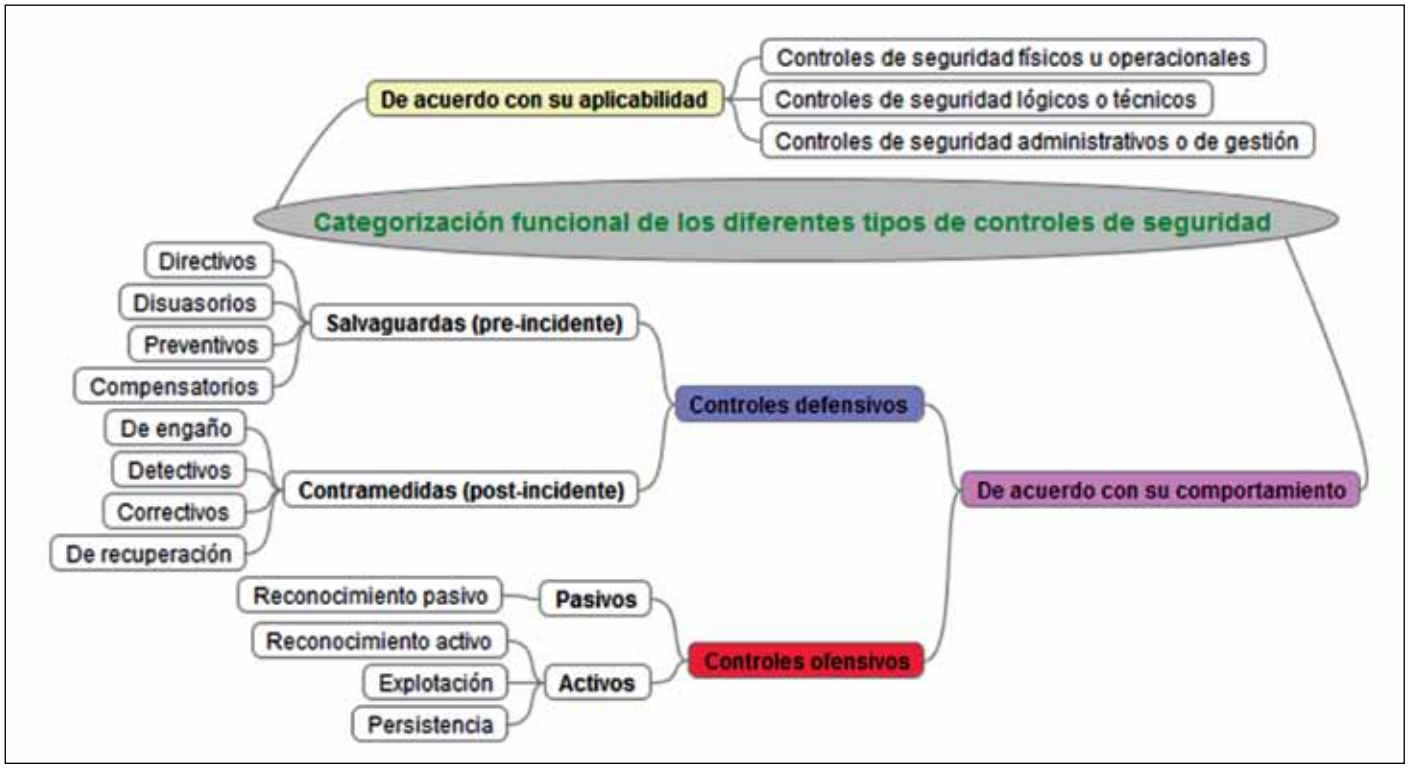

Figura 1

actividades es responsabilidad del **Equipo Púrpura** ("Purple Team"), compuesto por el responsable de seguridad de la información de la organización y personal del área de auditoría interna.

Controles defensivos

Este tipo de controles están orientados hacia la protección de los activos de información de la organización ante cualquier amenaza. Su función suele ser pasiva, ya que las actividades que desarrollan se focalizan en la preparación y respuesta ante la ocurrencia de un potencial incidente. Su gestión está bajo la responsabilidad del **Equipo Azul** ("Blue Team"), compuesto por el personal de seguridad de la información de la organización y los equipos de operación y administración.

A su vez, los controles defensivos se pueden organizar en dos subgrupos dependiendo del momento en el cual podrán actuar: **Salvaguardas y contramedidas**. La línea que hace esta separación es el momento de la ocurrencia de un incidente de seguridad:

– **Salvaguardas**: En este subgrupo se encuentran los diferentes controles implementados para gestionar, prevenir y disuadir cualquier potencial amenaza **antes** de que se materialice. En este grupo se encuentran los siguientes tipos de controles:

• **Directivos**: Controles que permiten la especificación de un modelo de reglas que definirán el comportamiento esperado y aceptado en términos de seguridad en la organización (lo qué se puede hacer y lo qué no), así como las acciones de defensa relacionadas.

Ejemplos:

· Políticas de seguridad

· Acuerdos de confidencialidad.

• **Disuasorios**: Controles cuyo objetivo está en inducir a un potencial atacante para que desista de su propósito. Su marco de acción suele ser fundamentalmente psicológico.

Ejemplos:

· Avisos de advertencia

· Cámaras de videovigilancia inactivas

• **Preventivos**: Este tipo de controles son la primera línea de acción frente a una posible amenaza. Por lo general están enfocados en la aplicación de restricciones para evitar un riesgo de forma anticipada.

Ejemplos:

· Vallas de seguridad

· Cortafuegos ("firewalls")

· Formularios de autenticación

• **Compensatorios**: Controles alternativos que se usan cuando existe una restricción técnica o del negocio justificada que no permite la implementación de un control específico de acuerdo con lo que indican los lineamientos directivos.

Ejemplos:

· Control de software malicioso a través de listas blancas ("whitelists")

· Supervisión adicional a las tareas de los empleados.

– **Contramedidas:** En este subgrupo se encuentran aquellos controles cuyo objetivo es identificar, detener, contener y corregir una amenaza cuando ésta ya se ha materializado. En este grupo se encuentran los siguientes controles:

• **De engaño**: Controles señuelo que permiten desviar la atención de un potencial atacante hacia un objetivo configurado intencionalmente de forma insegura para que pueda ser atacado, pero que se encuentra aislado y monitorizado por la organización. Esto permite contener y analizar las acciones del atacante mientras que se optimizan las propias defensas.

Ejemplos:

· Honeypots y honeynets

· Cajas fuertes vacías.

• **Detectivos**: Controles que permiten proveer una notificación al personal encargado cuando el incidente ya ha ocurrido o se han detectado comportamientos anormales que pueden ser indicios de la

ocurrencia de un incidente.

Ejemplos:

· Registros de eventos ("logs")

· Sensores de movimiento

· Sistemas de Detección de Intrusos ("Intrusion Detection Systems" – IDS)

• **Correctivos**: Este tipo de controles están orientados a la contención del daño y la reconfiguración de los activos afectados.

Ejemplos:

· Extintores de fuego

· Terminación de conexiones

· Finalización del contrato.

• **De recuperación**: Finalmente, este tipo de controles permiten que el activo pueda retornar a la operación normal, corrigiendo cualquier daño causado por el incidente.

Ejemplos:

· Copias de seguridad ("backups")

· Uso de centros de procesamiento de datos alternativos

Es importante resaltar que estas categorías no son necesariamente excluyentes. Es decir: un control puede operar bajo una o múltiples categorías. Por ejemplo, un sistema de prevención de intrusiones ("Intrusion Prevention System" – IPS) es un control defensivo de tipo detectivo (ya que genera una notificación del ataque) y correctivo (ya que permite la finalización de la conexión maliciosa y el bloqueo de conexiones subsiguientes).

Controles ofensivos

Este tipo de controles permiten la evaluación proactiva de la postura de seguridad corporativa y la mejora continua de los niveles de seguridad ofrecidos por los controles defensivos implementados en la organización. Su naturaleza es activa y se basa en la generación de incidentes reales o simulados, emulando las técnicas que podrían usar los atacantes de la forma más real posible. Su ejecución debe ser explícitamente coordinada por la organización y dentro de unos límites específicos. Igualmente, no puede ser ejecutada contra organizaciones externas a menos de que se tenga una aprobación.

La gestión de este tipo de controles recae en el **Equipo Rojo** ("Red Team"), que puede estar compuesto por personal interno o externo que garantice independencia del equipo azul. Dependiendo de las limitaciones en términos de tiempo de las pruebas y el realismo de los resultados, el equipo rojo puede tener o no conocimiento del entorno defendido.

Estos controles se pueden subdividir en **pasivos** y **activos**, dependiendo de la activación o no de una acción que viole explícitamente los controles defensivos (incidente):

– **Pasivos**: Controles que de forma explícita no violan ningún control defensivo, con lo cual sus acciones no se pueden catalogar como incidentes.

• **Reconocimiento pasivo**: Este tipo de controles se enmarcan en la realización de acciones aceptables dentro del marco normativo de la organización, pero cuyos resultados pueden ofrecer datos al equipo rojo para perfilar sus acciones.

Ejemplos:

· Analizadores del espectro electromagnético

· Capturadores de tráfico ("sniffing")

· Ingeniería social

– **Activos**: A diferencia de los controles pasivos, estos controles infringen explícitamente una política de seguridad y pueden afectar la integridad, confidencialidad y/o disponibilidad de los activos, por lo cual deben ser gestionados de forma muy controlada para minimizar posibles errores.

• **Reconocimiento activo**: Estos controles permiten la detección de posibles vulnerabilidades en los sistemas defensivos mediante la ejecución de pruebas simuladas.

Ejemplos:

· Escaneadores de vulnerabilidades.

· Auditorías técnicas de sistemas.

· Simulacros de planes de respuesta a incidentes.

• **Explotación**: Estos controles están orientados a la utilización de una vulnerabilidad previamente identificada en un control defensivo para aprovecharse de ella y lograr un objetivo definido.

Ejemplo:

· Herramientas para pruebas de penetración.

• **Persistencia**: Estos controles permiten la continuidad y subsistencia de los privilegios y accesos obtenidos con posterioridad a la vulneración del activo.

Ejemplos:

· Controles anti-forenses

Conclusión

El área de seguridad de la información (que comprende la dimensión física, lógica y administrativa) contempla la interacción entre controles de seguridad ofensivos y defensivos, cuyo objetivo es la protección continua de los activos de la organización.

Posterior a la ejecución de un análisis de riesgos que permita la identificación de activos y su valoración, así como las amenazas, vulnerabilidades, frecuencia e impacto, el paso siguiente es la elección de los controles de seguridad para gestionar dichos riesgos. Esta estrategia parte de la premisa del conocimiento de los tipos y categorías de los controles de seguridad disponibles para que se pueda realizar su despliegue óptimo con base en un criterio de coste-beneficio para la organización.

La coordinación entre los controles defensivos y ofensivos de la organización y la aplicación de acciones de mejora continua con base en los resultados de sus actividades es responsabilidad del "Purple Team", compuesto por el responsable de seguridad de la información de la organización y personal de auditoría interna.

La optimización de los controles defensivos se basa en la existencia de su contraparte: los controles ofensivos. Mediante esta interacción, la organización podrá monitorizar la efectividad y eficiencia de su estrategia, obtener evidencias e indicadores claves para la mejora continua y alinear los niveles de seguridad con base en las necesidades del negocio. ■

David E. Acosta Rodríguez
Consultor Senior en Seguridad
CISSP Instructor, CISM, CISA, CRISC,
CHFI Instructor,
CEH, PCI QSA, QSA(P2PE), 3DS
Assessor, OPST, BS25999 L.A.
INTERNET SECURITY AUDITORS