Clasificación de Controles Claves en la Seguridad de los Sistemas de Información

1 Introducción: ¿Qué es un control en sistemas de información?

En el ámbito de la seguridad de los sistemas de información, el término control se refiere a cualquier medida técnica, administrativa o física diseñada para preservar los principios fundamentales de la seguridad de la información: la confidencialidad, la integridad y la disponibilidad (conocidos como la tríada CIA por sus siglas en inglés: **Confidentiality, Integrity, Availability**).

Un control busca proteger los activos informáticos frente a amenazas internas o externas, asegurando que los procesos se ejecuten conforme a las políticas de seguridad definidas por la organización.

Existen diversas formas de implementar controles, que pueden ir desde mecanismos físicos, como sistemas de detección y extinción de incendios o el resguardo de materiales peligrosos, hasta procedimientos organizativos, como la segregación de funciones, el respaldo de datos y los mecanismos de control de acceso a áreas restringidas.

En función de su propósito y momento de actuación frente a un incidente, los controles se clasifican en preventivos, detectivos, correctivos y recuperatorios.

2 Controles preventivos: la primera línea de defensa

Los controles preventivos constituyen el primer nivel de protección en un sistema de información. Su objetivo principal es impedir que ocurran eventos que puedan afectar la confidencialidad, integridad o disponibilidad de los activos informáticos. Estos controles buscan reducir la probabilidad de errores, omisiones o acciones maliciosas, guiando el comportamiento de los usuarios y promoviendo la correcta ejecución de los procesos.

En general, se trata de controles de carácter pasivo, es decir, que no reaccionan directamente ante un incidente, sino que están diseñados para evitar que estos ocurran. Entre las medidas más comunes se encuentran la definición clara de responsabilidades, la selección y capacitación del personal, la

estandarización de procedimientos, la separación y rotación de tareas, el uso de contraseñas y tarjetas de identificación, y la implementación de firewalls o software de control de acceso. También forman parte de este grupo los formularios pre numerados, las máscaras de entrada de datos y las políticas y estándares documentados que regulan el uso del sistema.

La fortaleza de los controles preventivos radica en su capacidad para anticiparse a los riesgos y establecer un entorno de seguridad proactivo, donde los errores se minimizan y las conductas inseguras se desalientan desde el diseño mismo de los procesos.

3 Controles detectivos: monitoreo y visibilidad del riesgo

Cuando un incidente no ha podido ser evitado por los controles preventivos, entran en juego los controles detectivos. Estos mecanismos están diseñados para identificar y reportar errores, omisiones o actos maliciosos una vez que se han producido. Su función es monitorear los procesos, registrar las anomalías, detectar patrones inusuales de comportamiento y alertar a los responsables sobre la ocurrencia de eventos que puedan comprometer la seguridad de la información.

Los controles detectivos no corrigen los errores, pero generan evidencia de su existencia, lo que permite a la organización investigar las causas y activar las respuestas adecuadas. Entre los controles más representativos se incluyen los registros de acceso (logs), las auditorías de sistemas, los sistemas de detección de intrusos (IDS), el control de secuencias de procesos, la reconciliación de cuentas, la verificación cruzada de datos, la numeración de lotes, el control de validez, y los totales de control y pendientes.

Asimismo, es importante señalar que algunos controles como la capacitación en seguridad o la percepción organizacional de la importancia de los datos pueden cumplir tanto funciones preventivas como detectivas, al ayudar a identificar posibles violaciones o anomalías antes de que escalen a eventos críticos.

El valor de los controles detectivos radica en su capacidad para brindar visibilidad sobre lo que ocurre en el sistema, identificar fallos en los controles anteriores, y permitir la trazabilidad de las acciones que derivaron en una falla o incidente.

4 Controles correctivos: remediación y continuidad operativa

Una vez detectado un error o evento adverso, los controles correctivos intervienen para restaurar el estado normal del sistema, mitigar los efectos del incidente y corregir sus causas inmediatas. Estos controles permiten reprocesar operaciones afectadas, actualizar registros erróneos y restablecer servicios interrumpidos, con el objetivo de minimizar el impacto en la organización.

Entre los mecanismos correctivos más utilizados se encuentran la corrección automática de errores, las estadísticas sobre fuentes de error, los listados de discrepancias, las pistas de auditoría posteriores al incidente, y el respaldo operativo. Estos controles suelen tener un costo mayor debido a la intervención que requieren y a la necesidad de validar nuevamente los datos procesados.

A diferencia de los controles preventivos, que buscan evitar errores, y los detectivos, que buscan identificarlos, los correctivos asumen que el error ha ocurrido y se concentran en restaurar el sistema a un estado funcional. Su eficacia está directamente vinculada a la capacidad del sistema para reaccionar ante imprevistos y adaptarse a situaciones de emergencia.

5 Controles recuperatorios: restauración de servicios y resiliencia

Una categoría particular dentro de los controles correctivos son los controles recuperatorios. Aunque comparten con los correctivos el hecho de actuar a posteriori, su foco está puesto en restaurar rápidamente los servicios críticos afectados y facilitar la investigación posterior del incidente.

Los controles recuperatorios incluyen procedimientos como los respaldos de datos, el soporte técnico disponible 24/7, los planes de contingencia, y el plan de continuidad del negocio. Estos elementos son esenciales para asegurar que, en caso de catástrofes o incidentes graves, la organización pueda seguir operando, proteger la integridad de su información y recuperar los servicios esenciales en el menor tiempo posible.

Su implementación requiere una planificación estratégica, pruebas periódicas, actualización constante y la participación coordinada de múltiples áreas de la organización. La ausencia de controles recuperatorios puede derivar en pérdidas irreversibles de datos, interrupciones prolongadas y daños reputacionales significativos.

6 Consideraciones finales: la jerarquía de los controles

En el diseño de una estrategia integral de seguridad, se considera que el mejor control es aquel que impide la ocurrencia del problema: los controles preventivos. En segundo lugar se valoran los controles detectivos, ya que permiten reconocer cuándo algo ha fallado y tomar medidas de investigación o alerta. Finalmente, se ubican los controles correctivos y recuperatorios, que si bien son esenciales, actúan una vez que el daño ya ha ocurrido.

Un sistema de seguridad eficaz debe combinar de forma inteligente los distintos tipos de controles, de modo tal que actúen en forma complementaria, cubriendo todas las etapas del ciclo de vida de los incidentes: **prevención, detección, corrección y recuperación**. Solo así se puede garantizar una protección robusta de los activos de información frente a un entorno cada vez más complejo y cambiante.