fidélitas

Virtual

Semana

04

Curso Virtual

Auditoría de Sistemas

Clase sincrónica

Auditoría de sistemas basada en riesgos

Auditoría de sistemas basada en riesgos

fidélitas Virtual

Gestión de riesgos

¿Qué es?

La gestión de riesgos es el proceso de identificar las vulnerabilidades y las amenazas para los recursos de información utilizados por una organización para lograr los objetivos de negocio, y decidir que contramedidas (protecciones o controles) tomar, si hubiera alguna, para reducir el riesgo a un nivel aceptable (es decir, riesgo residual), basándose en el valor del recurso de información para la organización. (ISACA, 2011)

Auditoría de sistemas basada en riesgos

fidélitas Virtual

¿Como se logra?

Amenazas: evitar, transferir, mitigar, aceptar.

Auditoría de sistemas basada en riesgos

fidélitas Virtual

Evitar
Cambiar las condiciones originales de ejecución del proyecto.

Transferir:
La gestión de riesgo es responsabilidad de otro.

Aceptar:
No cambiar el plan.

Mitigar:
Disminuir probabilidad o impacto.

Auditoría de sistemas basada en riesgos

- Evitar, por ejemplo, donde sea factible, escoger no implementar ciertas actividades o procesos que generen un riesgo (es decir, eliminar el riesgo al eliminar la causa).

- Mitigar, por ejemplo, definir, implementar y monitorear controles apropiados para reducir la probabilidad o el impacto del riesgo.

- Transferir (o asignar), por ejemplo, compartir el riesgo con socios o transferirlo mediante cobertura de seguros, acuerdo contractual u otros medios.

- Aceptar, es decir, reconocer formalmente la existencia del riesgo y monitorearlo.

Auditoría de sistemas basada en riesgos

fidélitas Virtual

Gestión del riesgo

Uno de los pasos del proceso de gestión de riesgos es la identificación y clasificación de los recursos o activos de información que necesitan protección porque son vulnerables a amenazas.

EI propósito de la clasificación puede ser priorizar investigaciones adicionales e identificar la protección apropiada (clasificación simple, basada en el valor del activo), o permitir la aplicación de un modelo estándar de protección (clasificación en términos de criticidad y sensibilidad). (ISACA, 2011)

Auditoría de sistemas basada en riesgos

fidélitas Virtual

Gestión del riesgo

En las organizaciones comerciales, las amenazas pueden ocasionar pérdidas financieras directas en el corto plazo o bien pérdidas financieras al final (indirecta) en el largo plazo.

Auditoría de sistemas basada en riesgos

Pérdida directa de dinero.

Violación de la legislación.

Pérdida de reputación.

Peligro potencial para el personal.

Pérdida de oportunidades de negocio.

Interrupción en las actividades de negocio.

Auditoría de sistemas basada en riesgos

fidélitas Virtual

Gestión de riesgos

En resumen, el proceso de gestión del riesgo debería lograr un balance efectivo en costo entre la aplicación de controles de seguridad como contramedidas y las amenazas significativas. Algunas de las amenazas están relacionadas con aspectos de seguridad que pueden ser extremadamente sensitivos para algunas industrias.

Auditoría de sistemas basada en riesgos

fidélitas Virtual

Controles de TI

Para que los sistemas de información concreten completamente las metas de optimización de beneficios, riesgos y recursos, se debe abordar el riesgo que podría prevenir o inhibir la obtención de estas metas. Las organizaciones diseñan, desarrollan, implementan y monitorean sistemas de información a través de políticas, procedimientos, prácticas y estructuras organizativas para abordar estos tipos de riesgos.

El ciclo de vida del control interno es de naturaleza dinámica y está diseñado para asegurar lógicamente que se alcancen las metas y los objetivos del negocio y de que se prevengan o detecten y corrijan los eventos no deseados.

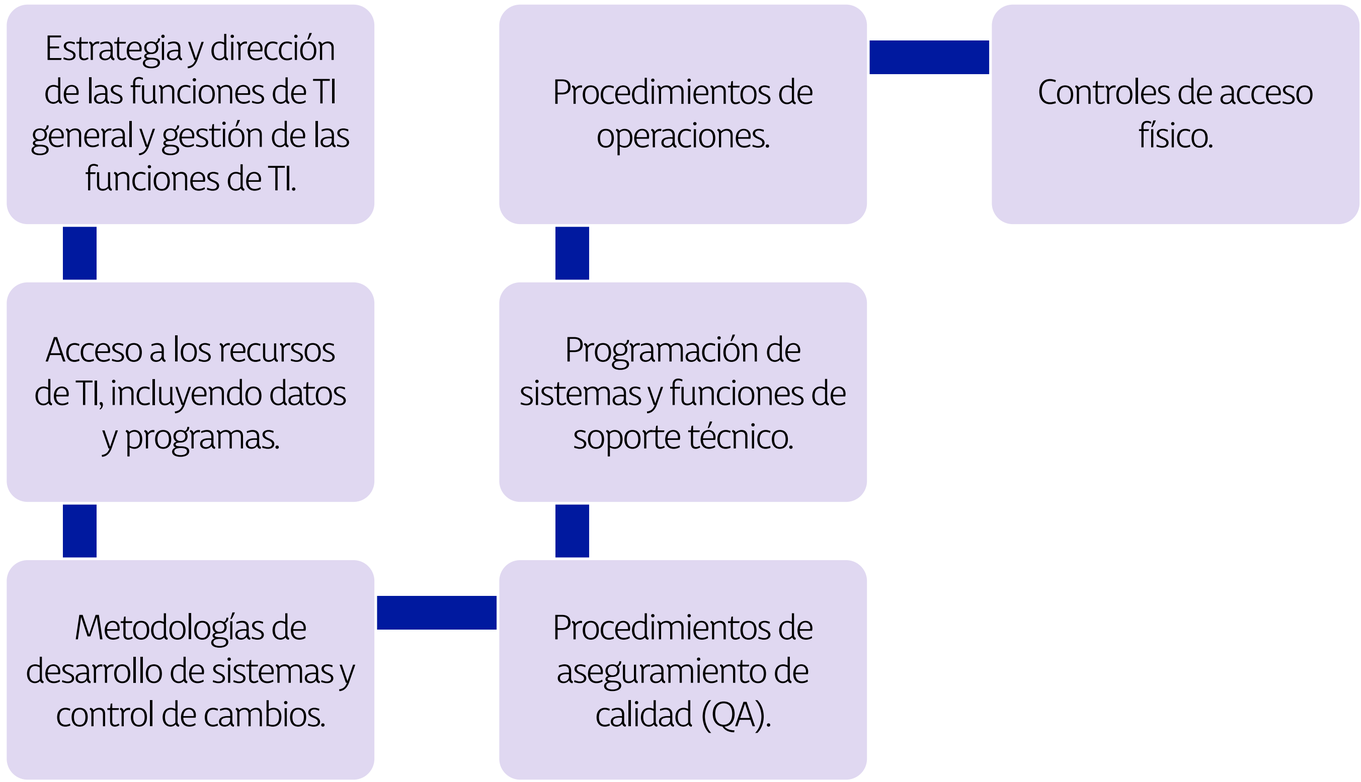
Auditoría de sistemas basada en riesgos

fidélitas Virtual

Cada control general puede ser traducido a un control específico de TI. Un sistema de información bien diseñado debería contar con controles construidos en el mismo para todas sus funciones sensitivas o críticas.

Auditoría de sistemas basada en riesgos

Procedimientos de control de un SI



Auditoría de sistemas basada en riesgos

Planificación de continuidad del negocio (BCP)/recuperación en caso de desastre (DRP).

Protección y mecanismos de detección contra ataques internos y externos.

Redes y comunicaciones.

Administración de la base de datos.

Auditoría de sistemas basada en riesgos

fidélitas Virtual

01 Después de que se han identificado los riesgos, se evalúan los controles existentes, o se valora si es necesario diseñar nuevos controles para reducir las vulnerabilidades a un nivel aceptable.

02 Estos controles se denominan contramedidas o salvaguardas e incluyen acciones, dispositivos, procedimientos o técnicas (es decir, personas, procesos o productos).

Auditoría de sistemas basada en riesgos

fidélitas Virtual

03 La fortaleza de un control puede ser medida en términos de su fortaleza inherente o de diseño y la probabilidad de su efectividad.

04 Para evaluar la solidez de un control se toma en cuenta su clasificación, si son preventivos, detectivos o correctivos, manuales o automatizados, y formales (es decir, se encuentran documentados en manuales de procedimientos y se mantienen pruebas de su operación) o *ad hoc*.

Auditoría de sistemas basada en riesgos

Tipos de control

Preventivos
Tratar de evitar o prevenir una acción.
Ejemplo: *software* de seguridad evita los accesos no autorizados.

Detectivos
Cuando fallan los preventivos para tratar de conocer cuanto antes el evento.
Ejemplo: registro de intentos de acceso no autorizados.

Correctivos
Facilitan la vuelta a la normalidad cuando se han producido fallas.
Ejemplo: recuperación de un archivo dañado a partir de las copias de seguridad.

Auditoría de sistemas basada en riesgos

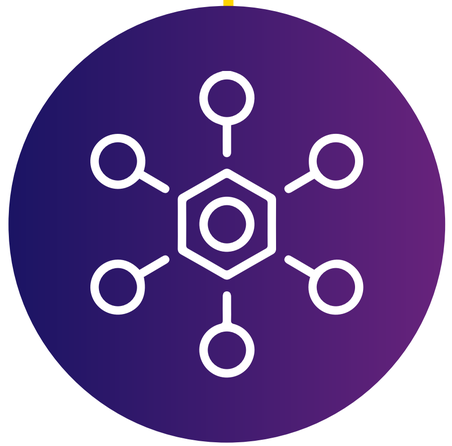
Clasificación del control

Clave	Función	Ejemplos
Preventivos	Detectan problemas antes de que aparezca, evita que ocurra un error o alto malicioso.	Documentos bien diseñados, segregaciones de funciones personal calificado.
Detectivos	Informan la ocurrencia del error.	Informes de cuentas vencidas, revisar registros, auditorías internas.
Correctivos	Minimiza el impacto de una amenaza, identifica la causa del problema.	Planes contingentes, procedimientos de respaldos.

Auditoría de sistemas basada en riesgos

fidélitas Virtual

Segregación de funciones



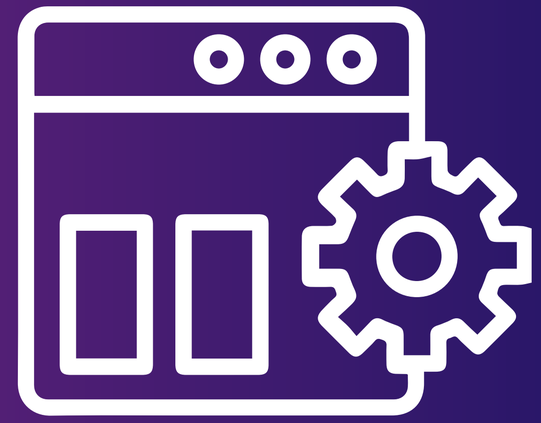
Su propósito es prevenir el fraude y los errores dividiendo las tareas y la autoridad para llevar a cabo un proceso entre varios empleados o gerentes. Si se requieren roles combinados, se deberían describir y aplicar los controles compensatorios según sea adecuado para la organización.

Auditoría de sistemas basada en riesgos

Cuando se asignan nuevos roles o se modifican los existentes, es importante garantizar que no se asignen roles incompatibles. Los roles deben revisarse periódicamente para prevenir una desviación de la función.

Auditoría de sistemas basada en riesgos

fidélitas Virtual



Controles compensatorios

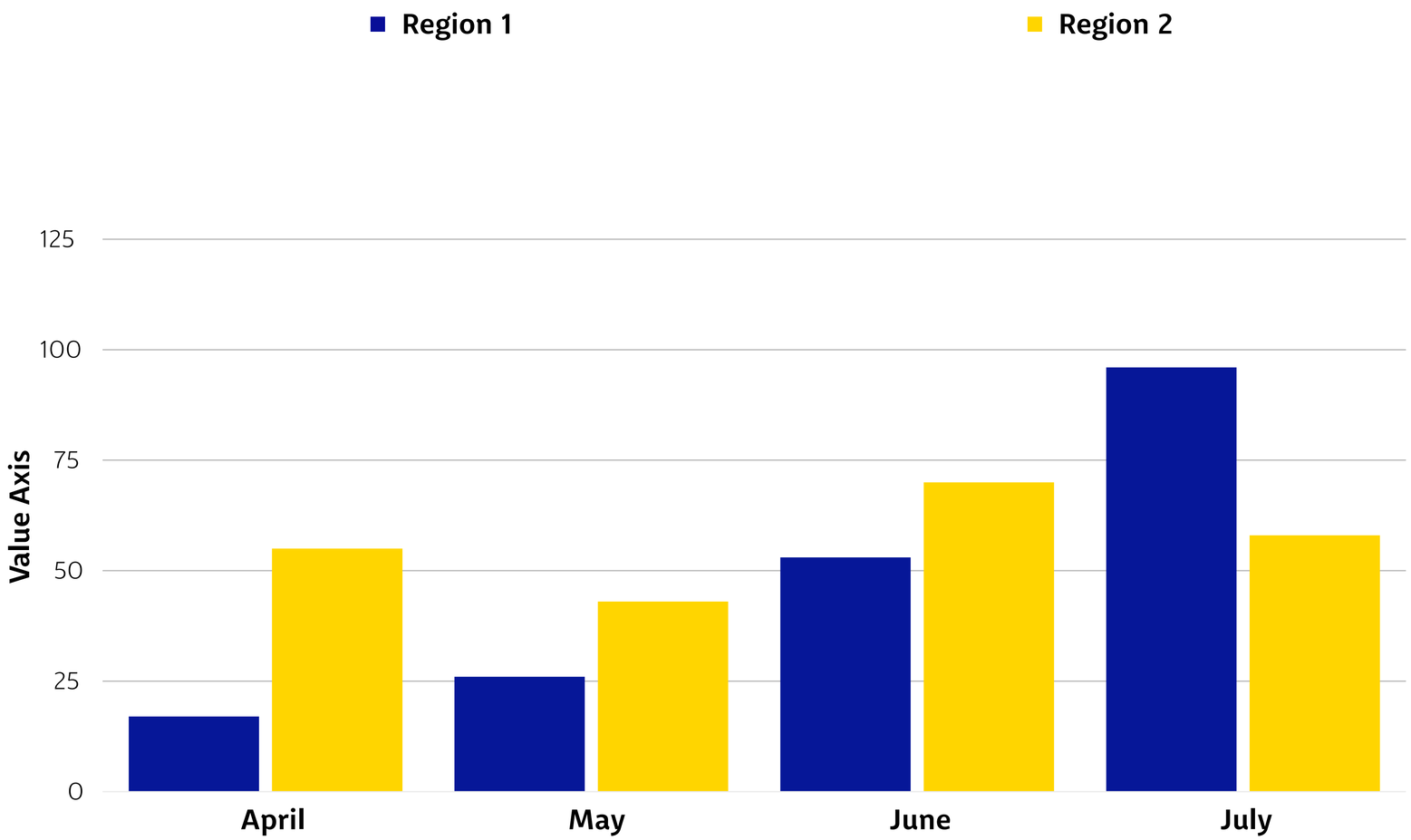
Controles compensatorios por falta de segregación de funciones: en negocios pequeños donde el departamento de SI puede estar constituido por solo 4 o 5 personas, debe existir medidas de control compensatorio para mitigar el riesgo resultante de una falta de segregación de funciones.

Auditoría de sistemas basada en riesgos

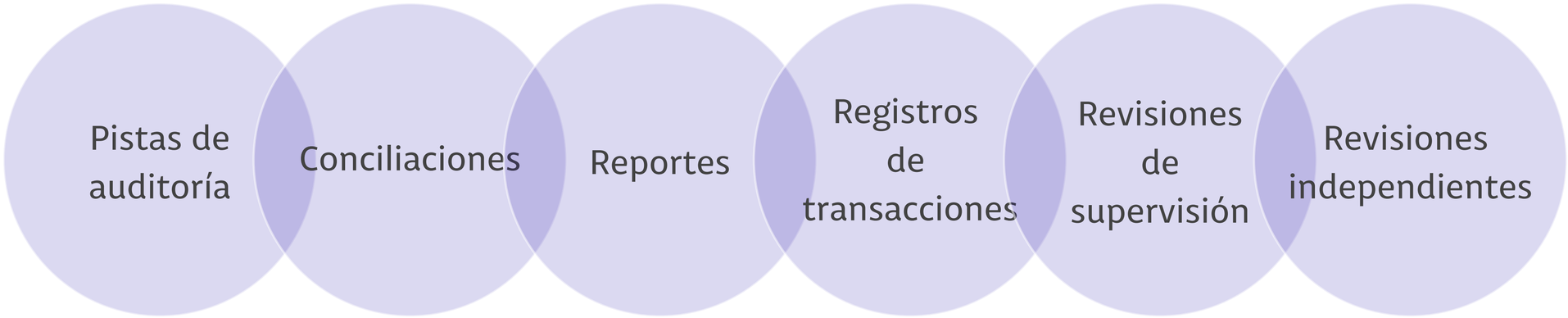
fidélitas Virtual

Antes de basarse en reportes generados por el sistema o en funciones como controles compensatorios, el auditor de SI debe evaluar cuidadosamente los reportes, las aplicaciones y los procesos relacionados con SI en busca de controles apropiados, incluyendo pruebas y controles de acceso para hacer cambios a los reportes o a las funciones.

Auditoría de sistemas basada en riesgos



Auditoría de sistemas basada en riesgos



Muchas gracias

fidélitas Virtual

Referencias bibliográficas

Andrés Álvarez, A. Fernández Sánchez, C. M. & Delgado Riss, B. (2020). Guía práctica de ISO/IEC 20000–1 para servicios TIC: (2 ed.). AENOR – Asociación Española de Normalización y Certificación. https://elibro.net/es/lc/ufidelitas/titulos/131803

Kegerreis, M., Schiller, M., & Davis, C. (2020). *IT Auditing Using Controls to Protect Information Assets*, Third Edition /. Mcgraw–Hill Education.

Referencias bibliográficas

Fernández Sánchez, C. M. (2012). Modelo para el gobierno de las TIC basado en las normas ISO: (ed.). AENOR – Asociación Española de Normalización y Certificación. https://elibro.net/es/lc/ufidelitas/titulos/53581

Piattini Velthuis, M. (2015). Auditoría de tecnologías y sistemas de información: (ed.). RA-MA Editorial. https://elibro.net/es/lc/ufidelitas/titulos/106490

fidélitas

Virtual