Seguridad Operativa

INTRODUCCIÓN Y ANTECEDENTES

La seguridad operativa se enfoca más que nada en los procedimientos de operaciones y el desarrollo y mantenimiento de documentación, donde se definirá y documentará controles para la detección y prevención del acceso no autorizado y protecciones contra software maliciosos, esto para garantizar la seguridad de los datos y los servicios conectados a las redes de dicha organización.

Esto con la finalidad de poder verificar el cumplimiento de normas establecida en la organización, procedimientos y controles establecidos mediante evaluaciones y registros de actividades de los sistemas de datos que se vallan generando, teniendo como objetivo monitorear estados de riesgo en los sistemas y para el descubrimiento de posibles riesgos.

OBJETIVOS

- Evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.
- Garantizar que la información y las instalaciones de procesamiento de información estén protegidas contra el malware.
- Alcanzar un grado de protección deseado contra la pérdida de datos.
- Registrar los eventos relacionados con la seguridad de la información y generar evidencias.
- Garantizar la integridad de los sistemas operacionales para la organización.
- Evitar la explotación de vulnerabilidades técnicas.
- Minimizar el impacto de actividades de auditoría en los sistemas operacionales.

CONTROL DE REVISIÓN APLICABLES

Responsabilidades y procedimientos de operación	Realizar procedimientos para establecer las responsabilidades, gestiones y operación de todos los medios de información, para reducir riesgos de un mal uso del sistemas.	• Documentación de procedimientos de operación: Improvisaciones que pueden producir problemas o deficiencias en la realización del trabajo. • Gestión de cambios: Controlar los cambios que afectan a la seguridad de la información en la organización. • Gestión de capacidades: Monitorear y ajustar uso de recursos necesarios para garantizar el rendimiento adecuado en los sistemas en el futuro. • Separación de entornos de desarrollo, prueba y producción: Encargado de reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional.
Protección contra código malicioso	Los usuarios deben estar al tanto de los peligros de los que puedan surgir ya que toda información es vulnerable, para ello hay que tomar precauciones para evitar “malware” (virus informáticos) que conlleva a los robos, daños y destrucción de datos a los sistemas en la organización.	• Controles contra el código malicioso: Como seguridad se deben implementar programas para la detecciones de malware para detección, prevención de información en los sistemas en la organización.
Copias de seguridad	Establecer procedimientos rutinarios de respaldo y recuperación de información al igual que también requisitos de negocio "internos" de la organización. Un punto importante en una organización es decidir y establecer el tipo de almacenamiento, soporte a utilizar, frecuencia de copia y prueba de soportes.	• Copias de seguridad de la información: Realizar pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a reglas de respaldo convenida.
Registro de actividad y supervisión	La organización tendrá que cumplir con todos los requerimientos legales para que se lleve a cabo el monitoreo del sistema y el registro de actividades Para verificar la efectividad y la conformidad del modelo. La necesidad de implantar procesos de supervisión es más evidente ahora que la medición de la eficacia de los controles se ha convertido en un requisito	• Registro y gestión de eventos de actividad: Se deben producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información. • Protección de los registros de información: Se debe proteger contra posibles alteraciones y accesos no autorizados la información de los registros. • Registros de actividad del administrador y operador del sistema: Registrar, proteger y revisar las actividades del administrador y del operador del sistema de

	específico.	manera regular. • Sincronización de relojes: Todos los sistemas de procesamiento de información dentro de una organización o de un dominio de seguridad deben ser sincronizados a una fuente de sincronización única de referencia.
Control del software en explotación	Minimizar los riesgos de alteración de los sistemas de información implementando procedimientos que garanticen la seguridad y control, los cambios deben ser gestionados por personal autorizado, sobre todo Informar a las áreas usuarias antes de un cambio que pueda afectar sus operaciones.	• Instalación del software en sistemas en producción: Implementar un plan para controlar las instalaciones de programas en cada uno de los sistemas operativos de la organización.
Gestión de la vulnerabilidad técnica	Se verifican que los cambios sean gestionados por personal autorizado para efectuar un análisis de riesgos previo a los cambios en atención, aplicando medidas de respaldo y puntos de restauración que permitan retornar los sistemas al estado de estabilidad inicial con ciertas garantías.	• Gestión de las vulnerabilidades técnicas: Se obtiene la información sobre las vulnerabilidades de los sistemas, para posteriormente evaluar el grado de exposición y tomar las medidas necesarias para abordar los riesgos asociados. • Restricciones en la instalación de software: Implementar reglas de instalación de software por parte de cada uno de los usuarios de la empresa.
Consideraciones de las auditorías de los sistemas de información	Las evaluaciones de normas, controles y técnicas son muy importantes para lograr la confiabilidad y la seguridad que se procesa en los sistemas de información. Por ejemplo limitando las verificaciones a un acceso de "sólo lectura" en software tomando las medidas necesarias para contrarrestar los efectos de modificaciones.	• Controles de auditoria de los sistemas de información: Se tiene que planificar y acordar los requisitos y las actividades de auditoria que involucran la verificación de los sistemas operacionales,

PUNTOS DE APLICACIÓN

Los puntos de aplicación son los siguientes:

En las normas, procedimientos y controles establecidos mediante auditorías técnicas y registros de actividad de los sistemas como base para la monitorización del estado del riesgo en los sistemas y descubrimiento de nuevos riesgos.

Otra de las aplicaciones es en los controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados a las redes de la organización.