



¿Qué son los objetivos de control?

- Mecanismo para implementar procedimientos dentro de un sistema de información.
- Son utilizados para determinar objetivos específicos contra los cuales se evaluará la eficacia de los controles
- Deben ser claros y concisos ya que son la base para la implementación de la auditoría
- Son genéricos (independientes de plataforma técnica utilizada)
- Al estar orientados a procesos, permiten mejorar la ejecución de los mismos
- Definen las categorías de riesgo para un proceso o subproceso
- Existen estándares como COBIT que definen procesos genéricos para la gobernanza y administración de IT. Contiene principios cubriendo todos los aspectos de alto nivel de tecnología informática.
Se dividen en 4 dominios generales:
 - Planeamiento y Organización
 - Adquisición e Implementación
 - Entrega y Soporte
 - Monitoreo



Presentación del problema

- Organización de logística.
- Planta de 350 trabajadores.
- Recursos informáticos del centro de cómputos:
 - Servidor de dominio.
 - Gateway (para gestión de conexiones remotas).
 - Servidores de impresión, de aplicación y de archivos .
- Se utilizan computadoras y dispositivos móviles.
- El personal se conecta mediante VPN de forma remota.
- Según el cargo, responsabilidad y valor agregado, lo hacen mediante dispositivos provistos, o máquinas personales.
- Todo acceso queda registrado, y almacenado por (como mínimo) 6 meses.




Objetivos de control

- Control de uso de la VPN.
- Control de infraestructura de software de la empresa
- Control en la asignación de dispositivos a empleados.
- Control del uso de dispositivos asignados.
- Control de infraestructura del datacenter
- Control de acceso a los depósitos
- Control de resguardos de información (backups).




Control de uso de la VPN

- Control de horarios de conexiones a la vpn
- Control de ips origen de las conexiones
- Control de usuarios, credenciales y certificados digitales usados para el login a la VPN.
- Cantidad de transferencia asociada a cada conexión
- Control de destino del tráfico de la VPN. (solo a servidor de archivos, impresión y aplicación)



Control de infraestructura de software de la empresa

- Control de la política de backups de cada aplicación del datacenter
- Control de actualizaciones de versiones del software
- Control de licencias de software utilizadas
- Verificación de las políticas de acceso a los softwares por parte de los empleados
- Control del cumplimiento de políticas de historial (6 meses) de la empresa



Control en la asignación de dispositivos a empleados

- Control y registro de asignaciones asociadas al hardware (Jerarquía y Función) (Relojes biométricos, tarjeta magnética, celulares, computadoras, etc).
- Verificación del correcto funcionamiento de los dispositivos previa asignación
- Historial de mantenimiento/problemas de los dispositivos asignados



Control del uso de los dispositivos

- Control de horarios de conexión a la vpn.
- Control de acceso al servidor de Impresión. (cantidad de copias, documentos)
- Control de acceso al servidor de archivos y sus carpetas compartidas.
- Registro de las modificaciones a los archivos mediante versionado (historial de cambios).
- Registro de accesos a las aplicaciones dentro del Servidor de Aplicaciones. (autenticación centralizada usando oauth2 o saml)
- Control de operaciones permitidas dentro de cada aplicación (log de operaciones) y sus datos asociados dentro de cada aplicación.




Control de infraestructura del datacenter

- Verificación de las políticas de recambio de hardware
- Control del mantenimiento preventivo de discos
- Control de la vida útil de las baterías ups
- Verificación de infraestructura de soporte (refrigeración, limpieza de filtros de aire)



Control en el acceso a los depósitos

- Control de acceso físico biométrico de los empleados (horarios, validación)
- Control de los sistemas de vigilancia
- Control de stock de productos dentro de los depósitos



Control de resguardos de información en unidades externas (backups)

- Control de la realización de backups diarios
- Control sobre los usuarios encargados de realizar los backups
- Validación de los datos salvados
- Verificación del encriptado de backups
- Control de acceso a los backups
- Control del tiempo empleado en la realización de los backups