

El empleado hace aquello que se controla

Presentación del tema

En el ámbito organizacional, una premisa recurrente sostiene que “los empleados hacen aquello que los jefes controlan, no necesariamente aquello que los jefes declaran como importante”. Este principio, ampliamente estudiado en teoría administrativa y comportamiento organizacional, adquiere especial relevancia en el contexto de las Tecnologías de la Información (TI), donde la gestión efectiva depende de métricas, monitoreo y mecanismos formales de control.

En organizaciones digitalizadas, los sistemas de información (SI – Information Systems) permiten medir desempeño, cumplimiento normativo, productividad y seguridad. Sin embargo, lo que se mide y controla termina moldeando la conducta organizacional. Si la dirección controla únicamente indicadores financieros de corto plazo, los empleados optimizarán esos indicadores, incluso en detrimento de la seguridad informática, la calidad de datos o la sostenibilidad tecnológica.

Para estudiantes de licenciatura en administración, comprender este concepto implica analizar cómo los mecanismos de control influyen en la cultura digital, en la gestión de riesgos tecnológicos y en la alineación entre objetivos estratégicos y comportamiento operativo.

Desarrollo

Fundamento Teórico del Principio de Control

En teoría organizacional, el control constituye una de las funciones clásicas de la administración junto con la planificación, organización y dirección. El control implica:

Establecer estándares. Medir resultados. Comparar desempeño. Aplicar correcciones. En entornos tecnológicos, estos estándares se traducen en:

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

Indicadores clave de desempeño (KPI – Key Performance Indicators). Acuerdos de Nivel de Servicio (SLA – Service Level Agreement). Auditorías de seguridad. Métricas de disponibilidad (Availability). Indicadores de cumplimiento normativo (Compliance). El comportamiento organizacional responde a incentivos y supervisión. Si la alta dirección controla la disponibilidad del sistema pero no controla la seguridad, el área técnica priorizará uptime (tiempo de actividad) sobre hardening (endurecimiento de seguridad).

La Relación entre Control y Cultura Digital

Los sistemas de información funcionan como instrumentos de vigilancia organizacional. Herramientas como:

ERP (Enterprise Resource Planning). CRM (Customer Relationship Management). SIEM (Security Information and Event Management). BI (Business Intelligence). permiten monitorear acciones individuales y colectivas.

Cuando la dirección controla sistemáticamente:

Accesos a sistemas. Tiempos de respuesta. Cumplimiento de protocolos de seguridad. Calidad de datos ingresados. los empleados internalizan esas prioridades.

En cambio, cuando no se audita el cumplimiento de políticas de seguridad informática, tienden a proliferar prácticas como:

Uso compartido de contraseñas. Descarga de software no autorizado. Almacenamiento de datos en dispositivos personales. Incumplimiento de políticas de respaldo (backup). La cultura digital no se construye únicamente con discursos estratégicos, sino con mecanismos de control efectivos y consistentes.

Control Formal vs. Control Informal

En TI, los controles pueden clasificarse en:

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

Controles Formales

Políticas documentadas. Procedimientos operativos. Auditorías internas. Evaluaciones de cumplimiento. Ejemplo: si se exige autenticación multifactor (MFA – Multi-Factor Authentication) y el sistema bloquea accesos sin este requisito, el comportamiento se alinea automáticamente.

Controles Informales

Supervisión directa. Cultura organizacional. Liderazgo ejemplar. Si los directivos ignoran protocolos de seguridad, el resto de la organización replicará esa conducta.

El Rol de las Métricas en TI

El principio “se hace lo que se controla” se intensifica en entornos digitalizados debido a la capacidad de medición automatizada.

Ejemplos de métricas que influyen en el comportamiento:

Tiempo promedio de resolución de incidentes (MTTR – Mean Time To Repair). Tasa de incidentes de seguridad. Porcentaje de cumplimiento de parches. Nivel de satisfacción del usuario. Si el único KPI del equipo de TI es reducir costos operativos, puede descuidarse la inversión en ciberseguridad.

Si se incorpora un indicador de reducción de vulnerabilidades, el equipo orientará esfuerzos hacia escaneos de seguridad y remediación.

Impacto en la Gestión de Riesgos

En gestión de riesgos tecnológicos, el control constante de:

Vulnerabilidades. Accesos privilegiados. Eventos de seguridad. Configuraciones críticas. reduce la exposición al riesgo.

Si la dirección no controla los accesos administrativos, aumentan las probabilidades de abuso de privilegios.

El concepto está estrechamente vinculado con el modelo de gobernanza de TI (IT Governance), que busca asegurar que las tecnologías soporten la estrategia organizacional.

Incentivos y Sistemas de Información

Los sistemas de información también estructuran incentivos.

Por ejemplo:

Si el CRM mide únicamente volumen de ventas, el equipo comercial priorizará cantidad sobre calidad de datos. Si el ERP exige validación estricta de información financiera, los usuarios adoptarán mayor rigurosidad en el registro contable. El diseño del sistema actúa como mecanismo de control estructural.

Riesgos de un Control Mal Diseñado

Un exceso de control puede generar:

Burocratización. Reducción de innovación. Desmotivación. Un control insuficiente puede producir:

Incumplimiento normativo. Vulnerabilidades de seguridad. Pérdida de integridad de datos. El desafío administrativo radica en equilibrar eficiencia y supervisión.

Ejemplo Aplicado en Seguridad Informática

Supongamos que una empresa implementa una política de cambio obligatorio de contraseñas cada 90 días, pero no monitorea su cumplimiento.

Los empleados buscarán atajos.

Si el sistema impone automáticamente la renovación y bloquea accesos incumplidos, el comportamiento se ajusta.

Este ejemplo demuestra que el control efectivo debe estar integrado en la arquitectura tecnológica.

Relación con Gobierno Corporativo

Desde la perspectiva estratégica, el control en TI forma parte del marco de gobierno corporativo.

Modelos como:

COBIT (Control Objectives for Information and Related Technologies). ISO/IEC 27001 (Norma Internacional de Gestión de Seguridad de la Información). establecen estructuras formales para controlar procesos tecnológicos.

La ausencia de control debilita la alineación entre estrategia y operación.

Dimensión Ética y Responsabilidad

El principio también plantea cuestiones éticas:

¿Se controla lo relevante o solo lo cuantificable? ¿Se incentivan comportamientos responsables o meramente productivos? En entornos digitales, medir únicamente productividad sin medir seguridad puede generar incentivos perversos.

Conclusión

El concepto de que “los empleados hacen lo que les controlan los jefes” representa una verdad organizacional particularmente significativa en el ámbito de las tecnologías de la información. Los sistemas digitales permiten medir, auditar y monitorear casi todas las actividades operativas, por lo que los indicadores seleccionados determinan el comportamiento organizacional.

En el contexto de TI, el control efectivo influye en:

Seguridad informática. Calidad de datos. Cumplimiento normativo. Gestión de riesgos. Eficiencia operativa. Para los futuros administradores, comprender este principio implica reconocer que el diseño de métricas, controles y sistemas de información no es neutro: configura la cultura organizacional y orienta la conducta de los empleados. El desafío estratégico consiste en controlar aquello que verdaderamente preserva el valor de la

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

información y la sostenibilidad del negocio, evitando tanto el exceso como la ausencia de supervisión.

Conceptos clave

- El empleado hace aquello que se controla
- Tecnologías de la Información (TI)
- Sistemas de Información (SI)
- Planificación de Recursos Empresariales (ERP)
- Gestión de Relaciones con Clientes (CRM)
- Inteligencia de Negocios (BI)
- Autenticación multifactor (MFA)
- Gestión de información y eventos de seguridad (SIEM)

Preguntas de repaso del tema

1. ¿Por qué los indicadores de desempeño influyen directamente en el comportamiento de los empleados?
2. ¿Cómo puede un sistema ERP funcionar como mecanismo de control organizacional?
3. ¿Qué riesgos surgen cuando no se controlan los accesos privilegiados en TI?
4. ¿Cuál es la relación entre gobierno de TI y mecanismos de control?
5. ¿Cómo puede un administrador equilibrar control, innovación y eficiencia en entornos digitales?
6. ¿Qué función cumplen los controles dentro de la gestión de riesgos tecnológicos?

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

7. ¿Cómo se diferencian los controles preventivos, detectivos y correctivos?
8. ¿Por qué los controles deben alinearse con los objetivos del negocio?
9. ¿Qué consecuencias puede generar la ausencia de controles documentados?
10. ¿Cuál es el concepto central de El empleado hace aquello que se controla dentro de la Gestión de Tecnologías Digitales?