CAMARA DE COMERCIO DE SANTIAGO

2024

RECOMENDACIONES DE CIBERSEGURIDAD

PARA PEQUEÑAS Y MEDIANAS EMPRESAS

Disclaimer

Los estudios, puntos de vistas y/o recomendaciones publicadas por la Cámara de Comercio de Santiago (CCS) son trabajos de investigación en curso y no deben ser considerados como definitivos o concluyentes.
Las opiniones expresadas en los mismos son responsabilidad exclusiva de los autores y no reflejan necesariamente la opinión oficial de la CCS.
La CCS no se hace responsable de la exactitud o veracidad de la información contenida en los mismos.
La CCS no se hace responsable de los daños o perjuicios que puedan derivarse del uso de la información contenida en los mismos.

Comité de Ciberseguridad de la Cámara de Comercio de Santiago (CCS)

Objetivo

El Comité de Ciberseguridad de la CCS tiene como objetivo generar una red de colaboración entre empresas socias de la CCS, a partir de la cual puedan:

- Compartir experiencias y buenas prácticas en materia de ciberseguridad.
- Desarrollar proyectos de fortalecimiento de sus áreas de TI/Ciberseguridad.
- Apoyarse para enfrentar y prevenir ciberataques o delitos informáticos.
- Asegurar la continuidad de sus operaciones.

Integrantes:

El Comité de Ciberseguridad está conformado por Nicolás Corrado, presidente del Comité, Yerka Yukich, directora ejecutiva, Daniela Cisternas, coordinadora del Comité y compuesto por representantes de empresas socias de la CCS que tienen experiencia en el ámbito de la ciberseguridad. A la fecha del presente documento los representantes son:

- Andrés Matus
- Iván Griman
- Marco Arriarán
- Mauricio Cantergiani
- Rafael Huerta
- Sebastián Izquierdo
- Shirley Hernández
- Walter Adorno
- Wilson España

3. Actividades:

El Comité de Ciberseguridad realiza diversas actividades, entre ellas:

- Reuniones periódicas para compartir experiencias y buenas prácticas.
- Seminarios y talleres sobre temas de ciberseguridad.
- Publicación de estudios y documentos sobre ciberseguridad.
- Desarrollo de proyectos de colaboración entre empresas socias.

4. Beneficios:

Las empresas que participan en el Comité de Ciberseguridad pueden obtener diversos beneficios, entre ellos:

- Acceso a información actualizada sobre las últimas amenazas y tendencias en materia de ciberseguridad.
- Oportunidad de compartir experiencias y buenas prácticas con otras empresas.
- Desarrollo de relaciones de colaboración con otras empresas.
- Fortalecimiento de sus áreas de TI/Ciberseguridad.
- Mejora de su capacidad para enfrentar y prevenir ciberataques.
- Mejora de su capacidad en la identificación de riesgos, de manera de diseñar e implementar controles que no permitan la materialización de amenazas en esta materia.

5. Cómo participar:

Las empresas socias de la CCS que estén interesadas en participar en el Comité de Ciberseguridad pueden hacerlo contactando a la Secretaría Ejecutiva del Comité.

6. Información adicional:

Sitio web del Comité de Ciberseguridad:
https://www.ccs.cl/comité-de-ciberseguridad/

Contacto: Daniela Cisternas <dcisternas@ccs.cl>

Resumen Ejecutivo

Este memorando proporciona un marco integral de recomendaciones de ciberseguridad, siguiendo el modelo de Seguridad de Confianza Cero (Zero Trust), adaptado específicamente para las pequeñas y medianas empresas (PyMEs) en Chile.
En un escenario de digitalización acelerada y con una creciente sofisticación de ciberataques, se torna esencial que las PyMEs en Chile intensifiquen sus estrategias de seguridad digital, identificando nuevos riesgos que afecten a su entorno y conociendo los posibles controles que los mitiguen.
La ciberseguridad es vital para mantener la salud empresarial y el crecimiento económico, especialmente considerando que las PyMEs representan una porción significativa del tejido empresarial en América Latina, con un 11,1% de pequeñas empresas y un 88,4% de microempresas.
Durante 2022, los ataques de Compromiso de Correo Electrónico Empresarial (BEC) aumentaron en más de un 81%, afectando particularmente a las pequeñas empresas. Estos ataques se caracterizan por su ingeniería social y manipulación, donde los delincuentes utilizan información de fuentes abiertas para personalizar correos electrónicos y engañar a los empleados (1).

Además, los recientes ciberataques a proveedores de terceras partes, como el ransomware que afectó a una empresa que es proveedor de servicios digitales de Mercado Público en Chile, resaltan la importancia de la seguridad en la cadena de suministro. Este ataque no solo interrumpió el servicio de Mercado Público, sino que también afectó a otros organismos públicos y empresas privadas en Chile y varios países de Latinoamérica. Asimismo, una compañía de telecomunicaciones en el país, que provee servicios al gobierno chileno y otras empresas privadas y PyMES, sufrió un ataque que resultó en la indisponibilidad de algunos servicios públicos y privados, evidenciando cómo los ciberataques pueden tener ramificaciones extensas y perjudiciales para una variedad de personas y compañías. Ambos ataques afectaron tanto a empresas grandes así como a pequeñas y medianas empresas, siendo estás las más afectadas ya que un día sin poder vender o facturar afecta mucho más en la operación y reputación de dichas PyMes.

El enfoque de Confianza Cero (Zero Trust), que se centra en el principio de "nunca confiar, siempre verificar", es un modelo esencial para protegerse de manera holística contra amenazas internas y externas.

El presente documento se estructura en seis secciones claves, cinco de ellas basadas en dicho enfoque de Confianza Cero: Identidad, Datos, Endpoints, Workloads (Cargas de Trabajo) y Red y una sexta sección basado en las Personas dada la importancia que cada uno de nosotros tiene en la seguridad de la organización. Cada sección aborda un componente crítico de la infraestructura de TI y proporciona recomendaciones detalladas en tres áreas: Protección, Detección y Resiliencia.

Personas: Establece los criterios más importantes en que deben ser capacitados los colaboradores.

Identidad: La gestión de identidades digitales es fundamental en la estrategia de Confianza Cero para las PyMEs. Las recomendaciones se enfocan en fortalecer la autenticación, gestionar eficazmente los accesos y aumentar la conciencia de seguridad entre los usuarios. Se incluyen prácticas como la implementación de autenticación multifactor, gestión de contraseñas y capacitación de usuarios.

Datos: La protección de datos es crucial para cualquier empresa. Se sugieren métodos para clasificar y encriptar datos, controlar y monitorear el acceso y garantizar la integridad y disponibilidad de la información. Esto incluye el uso de encripción, controles de acceso basados en roles y estrategias de copia de seguridad.

Endpoints: Los dispositivos que acceden a la red organización representan puntos de entrada potenciales para amenazas. Las recomendaciones abarcan la instalación de sistemas de seguridad, la gestión de parches y la monitorización continua de estos dispositivos para detectar y responder a actividades sospechosas.
Cloud y Workloads (**Cargas de Trabajo**): Esta sección se centra en la protección de las aplicaciones y los servicios críticos para el negocio. Se incluyen estrategias para la gestión de la seguridad en la nube y la realización de pruebas de seguridad regulares. Recalcando en esta

instancia la importancia de proteger aun cuando se está utilizando clouds de hiper-escaladores o de otras empresas.

Red: La seguridad de la red es vital para evitar accesos no autorizados y proteger los recursos de la empresa. Se recomienda la implementación de firewalls, sistemas de prevención de intrusiones, monitoreo de red y estrategias de respuesta rápida a incidentes.
Cada sección del memorando ofrece un enfoque estructurado y detallado para mejorar la postura de seguridad de las PyMEs en Chile, proporcionando recomendaciones prácticas y efectivas en las áreas de protección, detección y resiliencia. Este enfoque integral no solo ayuda a prevenir incidentes de seguridad, sino que también asegura una respuesta efectiva y una rápida recuperación en caso de ataques, minimizando así el impacto en las operaciones empresariales.

Condiciones y Limitaciones al Alcance del Documento de Recomendaciones de Ciberseguridad para PyMEs en Chile

Este documento, centrado en proporcionar recomendaciones de ciberseguridad para pequeñas y medianas empresas (PyMEs) en Chile bajo el modelo de Seguridad de Confianza Cero, se sujeta a ciertas condiciones y limitaciones que son importantes considerar:

Contexto Específico de las PyMEs en Chile: Las recomendaciones están diseñadas considerando las características típicas y los recursos generalmente disponibles en las PyMEs chilenas. Podrían no ser completamente aplicables a organizaciones con circunstancias significativamente distintas en términos de tamaño, industria, o recursos tecnológicos y financieros.

Dinamismo del Entorno de Ciberseguridad: El campo de la ciberseguridad está en constante evolución, con nuevas amenazas y tecnologías emergiendo regularmente, como lo es en la actualidad la Inteligencia Artificial. Las recomendaciones pueden requerir actualizaciones periódicas para mantener su relevancia y efectividad.

Implementación y Gestión de Riesgos: La correcta implementación de estas recomendaciones depende de la capacidad de gestión de riesgos y recursos de cada empresa. Las limitaciones en estos aspectos podrían afectar la efectividad de las medidas propuestas.

Recurso Humano y Capacitación: La efectividad de muchas de estas medidas de seguridad depende en gran medida del factor humano. La falta de capacitación adecuada y continua del personal puede limitar la efectividad de las estrategias propuestas.

Costos y Recursos Financieros: La implementación de ciertas recomendaciones implica inversiones en tecnología, software y

capacitación. Las limitaciones financieras podrían restringir la adopción de algunas de las medidas sugeridas.

Cumplimiento Legal y Normativo: Las recomendaciones se ofrecen con la suposición de que las empresas cumplirán con todas las leyes y regulaciones locales e internacionales pertinentes. La adaptación a requisitos legales específicos puede requerir modificaciones en algunas de las estrategias sugeridas.

Tecnología y Infraestructura existentes: Las recomendaciones están formuladas suponiendo un cierto nivel de infraestructura tecnológica existente. Las empresas con infraestructuras tecnológicas significativamente diferentes podrían necesitar adaptaciones específicas.

Protección Integral: Aunque las recomendaciones buscan proporcionar un enfoque integral, no garantizan una seguridad completa. Las PyMEs deben estar preparadas para posibles brechas de seguridad a pesar de la implementación de estas medidas.

Riesgo Residual: Siempre existe un riesgo residual de seguridad, incluso con la implementación de las mejores prácticas. Las empresas deben estar conscientes de este hecho y tener planes de contingencia para responder a incidentes de seguridad.

Este documento debe considerarse como un punto de partida y una guía para mejorar la postura de seguridad de las PyMEs en Chile. Se recomienda que las empresas consulten con expertos en ciberseguridad para adaptar estas recomendaciones a sus necesidades y circunstancias específicas.

Personas

1. PROTECCIÓN – CONCIENTIZACION Y ENTRENAMIENTO:

1.1. Definir un plan de capacitación y concientización sobre riesgos de seguridad y buenas prácticas de ciberseguridad que alcance a todos los empleados.
1.2. Definir un programa de inducción para los nuevos colaboradores y capacitaciones periódicas para los ya existentes, que refuerce la concientización sobre ciberseguridad y las buenas prácticas.
1.3. Dicho programa o plan de capacitación debe contener aspectos como:
    1.3.1. Fomentar el uso de contraseñas fuertes y únicas, resaltando la importancia de estas y las constantes amenazas entorno a ellas.
    1.3.2. Entrenar acerca del uso de un gestor de contraseñas para almacenar las contraseñas de manera segura. Adicionalmente, explicar la importancia de la autenticación multifactor (MFA) y qué se debe hacer y qué no.
    1.3.3. Mantener actualizado el software y sistema operativo de todos los dispositivos (computadores, servidores, tablets y celulares)
    1.3.4. Riesgos de utilizar redes wifi-públicas o sin contraseña de acceso.
    1.3.5. Realizar copias de seguridad regulares de los datos importantes.
    1.3.6. El cuidado con los correos electrónicos y en la importancia de reconocer los phishing. No abrir correos de remitentes desconocidos ni hacer clic en enlaces sospechosos.
    1.3.7. La navegación segura evitando acceder a sitios web de dudosa reputación.
    1.3.8. La clasificación y protección de los datos, su criticidad y sensibilidad

1.4. Aclarar las responsabilidades de cada rol dentro de la organización según la accesibilidad a los activos que maneja.
1.5. Se recomienda que las buenas prácticas sean parte del reglamento interno de la empresa y sea un anexo al contrato de trabajo.
1.6. La dirección de la empresa debe involucrarse en las iniciativas, impulsar, facilitar su implementación y velar por su cumplimiento.

Identidad

2. PROTECCIÓN:

2.1. Implementar autenticación multifactor (MFA) en todas las cuentas utilizando el bloqueo y monitoreo de geolocalización. Extendiendo el MFA a entornos personales, redes sociales, mail entre otros.
2.2. Establecer políticas de complejidad y renovación periódica de contraseñas y educar a los colaboradores los cuales pueden apoyarse en software gestores de contraseñas para mejorar la seguridad de las credenciales y no anotarlas en documentos sin encriptar.
2.3. Definir procesos de alta, baja y modificación (ABM) de cuentas para colaboradores, cuentas de servicios y bots.
2.4. Definir una nomenclatura estándar de las cuentas de usuario y mantener un inventario actualizado de las mismas asociándolas con las personas que las usan.
2.5. Verificar el cumplimiento de los procesos de ABM y nomenclatura sobre todo en el bloqueo/baja de cuentas de personas en el momento que dejan de trabajar en la organización.
2.6. Dar accesos a los usuarios según el criterio de mínimo necesario para su normal trabajo/funcionamiento, basado en modelos de accesos establecidos en roles (RBAC).
2.7. Limitar los privilegios de administrador y aplicar el principio de privilegio mínimo.
2.8. No utilizar cuentas genéricas.
2.9. Utilizar soluciones de Single Sign-On (SSO) para centralizar y controlar el acceso.

3. DETECCIÓN:

3.1. Monitorear y alertar sobre intentos de acceso sospechosos o fallidos.
3.2. Revisar regularmente los registros de acceso para detectar patrones anómalos.
3.3. Realizar auditorías periódicas de cuentas y accesos.
3.4. Realizar chequeos de postura verificando que las configuraciones de seguridad se encuentran correctamente definidas y no fueron modificadas.
3.5. Configurar alertas para cambios no autorizados en las configuraciones de seguridad.
3.6. Implementar soluciones de análisis de comportamiento de usuario.

4. RESILIENCIA:

4.1. Capacitar a los empleados en buenas prácticas de seguridad de identidades, como por ejemplo la importancia de no compartir claves y seleccionar contraseñas robustas, reconocer el phishing, etc.
4.2. Establecer un proceso claro de respuesta a incidentes relacionados con identidades comprometidas que permita el cambio de las contraseñas, el bloqueo y otras acciones que busquen contener un incidente.
4.3. Realizar simulacros de respuesta a incidentes de seguridad.
4.4. Implementar un proceso de recuperación de cuentas seguro incluyendo a los proveedores de las soluciones.
4.5. Mantener actualizadas las políticas de seguridad de identidad y acceso.

Endpoints

1. PROTECCIÓN:

1.1. Instalar y mantener actualizados antivirus, antimalware y firewalls en todos los dispositivos (computadores y servidores).
1.2. Implementar herramientas de detección y respuesta en endpoints: EDR - (Endpoint Detection and Response) o XDR (Extended Detection and Response).
1.3. Implementar políticas de actualización de software y parches de seguridad que permitan mantener actualizados los computadores aun cuando los mismos no estén en la red de la organización.
1.4. Realizar el cifrado de los discos en todas las computadoras utilizadas.
1.5. Asegurar la configuración segura (hardening) de dispositivos móviles y estaciones de trabajo que accedan a los datos de la empresa, como ejemplo, protectores de pantalla con contraseña que se activan automáticamente a los cinco minutos de inactividad.
1.6. Restringir el uso de dispositivos personales para actividades laborales (BYOD) o implementar controles estrictos para estos.
1.7. Definir controles mínimos de seguridad de dispositivos de terceras partes que accedan a los datos de la organización.
1.8. Utilizar soluciones de gestión de dispositivos móviles (MDM) para controlar y proteger los dispositivos y la información almacenada en ellos.

2. DETECCIÓN:

2.1. Activar los logs y monitorear el uso de dispositivos y aplicaciones para detectar actividades sospechosas.
2.2. Realizar auditorías regulares de seguridad de dispositivos para identificar vulnerabilidades.
2.3. Gestionar las consolas de las soluciones de protección y verificar la existencia de alertas.

2.4. Implementar soluciones de análisis de tráfico de red para identificar patrones anómalos.

3. RESILIENCIA:

3.1. Implementar el respaldo de los computadores en la nube y probarlo regularmente.
3.2. Establecer procedimientos claros de respuesta ante incidentes de seguridad en dispositivos, como por ejemplo ransomware.
3.3. Capacitar a los empleados en prácticas seguras de uso de dispositivos.
3.4. Mantener un inventario actualizado de todos los dispositivos y su estado de seguridad.
3.5. Desarrollar políticas para la rápida sustitución o reparación de dispositivos comprometidos.

Datos

1. PROTECCIÓN:

1.1. Clasificar y proteger los datos de la organización.
1.2. Identificar y clasificar los datos personales.
1.3. Encriptar los datos sensibles, tanto en reposo como en tránsito, ya sea en servidores propios como en la nube.
1.4. Implementar controles de acceso basados en roles para los datos.
1.5. Gestionar y restringir el acceso de terceras partes a datos de acuerdo con la clasificación de estos.
1.6. Realizar copias de seguridad regulares y seguras de datos importantes.
1.7. Controlar la expansión de los datos hacia muchos lugares, el dato debe estar igualmente protegido en todos lados.
1.8. Utilizar soluciones de prevención de pérdida de datos (DLP).
1.9. Implementar un sistema de gestión de derechos de información (IRM) como RMS para controlar el uso de los datos clasificados.

2. DETECCIÓN:

2.1. Monitorear el acceso y la transferencia de datos sensibles, dentro y fuera de la empresa.
2.2. Implementar herramientas para detectar anomalías en el manejo y transferencia de datos.
2.3. Realizar auditorías periódicas para identificar posibles exposiciones o mal manejo de datos.
2.4. Establecer alertas para modificaciones no autorizadas de datos.
2.5. Realizar el almacenamiento de los logs en fuentes externas por un mínimo de 90 días.

3. RESILIENCIA:

3.1. Definir cuál es el tiempo máximo que la organización puede funcionar sin determinados datos específicos y considerados críticos.

3.2. Desarrollar y mantener un plan de recuperación de datos que permita la recuperación en tiempos adecuados para la operación del negocio.
3.3. Realizar pruebas periódicas de restauración de datos.
3.4. Mantener un registro actualizado de la ubicación y el manejo de datos críticos.
3.5. Establecer procedimientos para responder a violaciones de datos y conforme a regulaciones y leyes.

Cloud y Cargas de trabajo

1. PROTECCIÓN:

1.1. Definir un gobierno y estrategia de protección del cloud (nube).
1.2. Establecer una matriz de responsabilidades claras entre el proveedor de cloud, la empresa y cualquier otro tercero posiblemente involucrado.
1.3. Evaluar impactos regulatorios al migrar al cloud.
1.4. Utilizar firewalls web (WAF) y sistemas de prevención de intrusiones para proteger las cargas de trabajo.
1.5. Aplicar la segmentación de red para aislar las cargas de trabajo críticas y asegurar los canales con servicios on-prem.
1.6. Implementar la configuración segura y la gestión de vulnerabilidades en servidores y aplicaciones del cloud.
1.7. Implementar políticas de acceso mínimo necesario para aplicaciones y servicios.

2. DETECCIÓN:

2.1. Activar los logs en servidores y aplicaciones (on-prem y cloud) y monitorear las cargas de trabajo para detectar actividades inusuales o sospechosas.
2.2. Analizar la posibilidad de integrar todos los logs a través de soluciones de centralizadas como SIEM y resguardar dichos logs en forma externa por períodos prolongados, preferentemente mayor a 90 días.
2.3. Realizar evaluaciones de vulnerabilidades, seguridad y pruebas de penetración regularmente en las aplicaciones y servicios.
2.4. Realizar auditorías periódicas de los registros y eventos de seguridad.
2.5. Utilizar herramientas de monitoreo de integridad para identificar cambios no autorizados.
2.6. Establecer alertas para modificaciones no autorizadas en aplicaciones y configuraciones.

2.7. Exigir reportes de seguridad al proveedor del cloud o de la solución as a service.

3. RESILIENCIA:

3.1. Desarrollar y mantener un plan de continuidad de negocio y recuperación ante desastres.
3.2. Capacitar al personal en procedimientos de recuperación y respuesta ante incidentes.
3.3. Analizar la posibilidad de establecer esquemas de resiliencia a través de multi-zonas de un mismo proveedor cloud o entre distintos proveedores de cloud (esquema de alta disponibilidad multi-cloud)
3.4. Realizar simulacros de respuesta a incidentes que afecten las cargas de trabajo.
3.5. Mantener copias de seguridad regulares y probadas de aplicaciones críticas.
3.6. Revisar y actualizar periódicamente las estrategias de resiliencia de las cargas de trabajo.

Red de Datos

1. PROTECCIÓN:

1.1. Implementar firewalls y sistemas de prevención de intrusiones para proteger la red.
1.2. Utilizar redes privadas virtuales (VPN) para el acceso remoto seguro.
1.3. Definir un segmento desmilitarizado (DMZ) para ubicar aquellos servicios que deban ser accedidos desde internet.
1.4. Asegurar la configuración de los dispositivos de red, incluyendo routers y switches.
1.5. Definir esquemas de control de accesos a la red (NAC)
1.6. Aplicar políticas de seguridad para el uso de redes inalámbricas y públicas.
1.7. Definir e implementar la segmentación o micro-segmentación de la red.

2. DETECCIÓN:

2.1. Realizar auditorías regulares de la infraestructura de red para detectar vulnerabilidades.
2.2. Utilizar sistemas de detección de intrusiones en red (NIDS) para monitorear el tráfico sospechoso.
2.3. Implementar soluciones de análisis de tráfico de red para identificar patrones anómalos.
2.4. Establecer un sistema de gestión y correlación de eventos de seguridad (SIEM) para un análisis integral.
2.5. Monitorear los registros de dispositivos de red para detectar actividades inusuales a través de un centro de operación 24x7 comúnmente conocido como SOC.

3. RESILIENCIA:

3.1. Desarrollar un plan de recuperación de redes y continuidad de operaciones.
3.2. Mantener una configuración de red redundante para asegurar la continuidad en caso de fallos.
3.3. Definir esquemas de doble proveedor para los enlaces críticos y última milla.
3.4. Implementar balanceadores de carga.
3.5. Establecer procedimientos de respuesta rápida a incidentes de seguridad de red.
3.6. Realizar pruebas periódicas de los planes de respuesta y recuperación de red.
3.7. Definir un comité de crisis.
3.8. Capacitar al personal en prácticas de seguridad de red y respuesta a incidentes.

Terminología

Seguridad de Confianza Cero (Zero Trust): Modelo de seguridad que opera bajo el principio de "nunca confiar, siempre verificar", enfocado en proteger los recursos de la organización independientemente de su ubicación.

Compromiso de Correo Electrónico Empresarial (BEC): Ataques de ingeniería social que buscan engañar a los empleados para que realicen transferencias de fondos o proporcionen información confidencial a gente fuera de la empresa.

Ransomware: Tipo de malware que cifra los archivos del usuario y exige un rescate para su desbloqueo.

Autenticación Multifactor (MFA): Método de seguridad que requiere dos o más pruebas de identidad independientes para verificar al usuario.

Gestión de Identidades Digitales: Procesos y tecnologías para gestionar y autenticar identidades digitales, incluyendo el control de accesos y la gestión de contraseñas.

Encripción de Datos: Proceso de convertir información en un código para prevenir accesos no autorizados.

Endpoints: Dispositivos finales como computadoras, móviles que se conectan a la red empresarial.

Workloads (Cargas de Trabajo): Se refiere a la cantidad de trabajo que se le asigna a un sistema informático en un momento dado en procesos y recursos, como por ejemplo para ejecutar aplicaciones o procesar datos.

Firewalls: Tecnología de seguridad de red diseñado para bloquear accesos no autorizados mientras permite comunicaciones autorizadas.

Sistemas de Prevención de Intrusiones (IPS): Dispositivos o aplicaciones de software que monitorean la red o los sistemas para actividades maliciosas.

Gestión de Vulnerabilidades: Proceso para identificar, clasificar, remediar y mitigar vulnerabilidades en los sistemas.

Resiliencia Cibernética: Capacidad de una organización para prepararse, responder y recuperarse de incidentes cibernéticos.

Riesgo: Existencia de una amenaza, o ciber-amenaza, que tenga consecuencias negativas para los sistemas de información de la empresa.