UNIVERSIDAD DON BOSCO
VICERRECTORÍA ACADÉMICA
FACULTAD DE INGENIERÍA

TRABAJO DE GRADUACIÓN PARA OPTAR AL GRADO DE

Maestro(a) en Seguridad y Gestión de Riesgos Informáticos

PROYECTO

Implementación de estándar CIS para escaneo de vulnerabilidades en granja de servidores Windows

PRESENTADO POR

Carlos Samuel Guzmán Barrientos GB212262

José Giovanni Viera López VL211678

ASESOR

Rene Humberto Rodríguez Mejía

Antiguo Cuscatlán, La Libertad, El Salvador, Centro América

Junio 2023

índice

Índice de imágenes

índice de Tablas

Objetivos

Objetivo general

Proteger los activos de información de las empresas Pyme por medio de la implementación de un proceso operativo de escaneo, categorización y remediación de vulnerabilidades a las que están expuestos los servidores Windows con base al estándar Critical Security Controls (CIS).

Objetivos específicos

a. Definir un proceso basado en la aplicación de Critical Security Controls (CIS) para reducir vulnerabilidades en la infraestructura tecnológica

b. Establecer la clasificación de vulnerabilidades y exposición mediante CVE (Common Vulnerabilities and Exposures)

c. Medir el nivel de riesgo a la que está expuesta la infraestructura tecnológica de la institución y definir las medidas remediales correspondientes

d. Analizar las normas de seguridad vigentes para que el marco de referencia se encuentre acorde a los lineamientos dictados por los estándares reconocidos de la industria.

Tipo de Investigación: Investigación Académica

Introducción

El presente proyecto de investigación busca establecer un marco de referencia para la implementación de controles críticos de seguridad (CIS-Center Of Internet Security) en una MiPymes, tomando en cuenta que la digitalización de los procesos en las organizaciones abre las puertas a nuevos riesgos en cuanto a la seguridad cibernética se refiere, esto obliga a las empresas a invertir en soluciones tecnológicas de protección digital y en recursos profesionales para crear y gestionar políticas de seguridad informática y herramientas de ciberseguridad, sin embargo, no todas las organizaciones pueden destinar los recursos económicos suficientes para cubrirse ante las amenazas digitales, también es importante considerar que debido a la pandemia de COVID-19 nació la necesidad de las empresas de todo tipo y tamaño de contar con los equipos tecnológicos para realizar teletrabajo, estas situaciones aumentan la probabilidad de ser víctimas de una intrusión cibernética y posteriores delitos informáticos.

Por lo cual, se pretende presentar la guía y marco de referencia de CIS el cual comienza a construirse desde el análisis de los antecedentes en términos de seguridad informática de la organización, de este análisis, se determina que no se puede garantizar que las pocas medidas de seguridad tomadas en la compañía cubran a todos los activos que debería proteger y peor aún se encuentren articulados entre ellos, esto implica que es necesario implementar los controles dictados por algún estándar de la industria, en este caso, se eligió la norma CIS, debido a que esta sugiere determinados puntos de control para pequeñas empresas que se encuentran en una etapa temprana de implementación de controles de seguridad informática, el desarrollo del marco de referencia busca proveer a las organizaciones las pautas claras a seguir al momento de implementar algún control de CIS y de esta manera pueda gestionar en un futuro su ciberseguridad con formalidad.

Justificación

El mundo se encuentra cursando el proceso llamado democratización del acceso a Internet, esto significa que conforme pasa el tiempo es más sencillo que las personas tengan acceso al mundo digital, y nuestro país no es la excepción.

Hoy en día la gente se encuentra hiperconectada, ya sea mediante sus computadores o sus dispositivos móviles, la presencia digital es prácticamente de 24 horas, no importa si se encuentran en su lugar de trabajo o en su hogar, las personas permanentemente se encuentran conectadas a la web.

Si las personas se encuentran hiperconectadas es lógico que las organizaciones también lo estén, esto implica que las instituciones corren los mismos riesgos que cualquier persona en Internet, porque detrás de todo proceso digital dentro de una empresa, siempre se encontrará una persona. Tarde o temprano las organizaciones llegan a la conciencia de comprender los riesgos y buscan protegerse, crean políticas de seguridad de la información, implementan herramientas digitales que protejan la infraestructura tecnológica y capacitan a su personal, todo esto genera una sensación de protección.

Por otro lado, ninguna medida de ciberseguridad es infalible, es aquí donde radica la importancia de implementar controles de seguridad informática, y hoy en día más que nunca, debido a que son más frecuentes las noticias de organizaciones víctimas de ataques cibernéticos. De acuerdo con un estudio de Kasperky las PYMES en Latinoamérica han sufrido 4 veces más ataques cibernéticos en los últimos 3 años (fuente - Las PyMEs de América Latina enfrentan un creciente número de ciberataques - kaspersky.com)

Los tres mayores delitos cometidos pueden traer consigo consecuencias tales como: el robo de credenciales de acceso a sistemas informáticos, robo de información, estafas electrónicas o instalación de software malicioso (malware) en los equipos informáticos, todas estas afectan de manera importante a personas y organizaciones, ocasionando pérdidas económicas, ya sea por el robo de dinero, la sustracción o pérdida de información o la imposibilidad de continuidad del negocio, sin mencionar el daño reputacional que las organizaciones sufren, para todo lo mencionado anteriormente, existen formas para defenderse de un ataque o reponerse de uno, sin embargo, no todas las organizaciones le brindan la importancia necesaria, debido a esto es importante implementar controles de seguridad informática para reducir los riesgos a los que se encuentran expuestos los activos y la información de las MiPymes.

Planteamiento de problemática

Situación de las Pymes en cuanto al tema de ciberseguridad

Liderazgo para crear cultura de la ciberseguridad

La ciberseguridad no debe ser aplicada exclusivamente a solo sistemas informáticos, sino que también es aplicable a personas.

Concientizar y capacitar a todos los empleados/as en protocolos de ciberseguridad, prevención de ciberataques, normativa regulatoria y bienestar digital es parte imprescindible del proceso de transformación digital y de una cultura en ciberseguridad.

Para implementar un plan de ciberseguridad en una organización es imprescindible capacitar a cada empleado/a según su relación con la tecnología corporativa.

Itinerarios formativos a medida de directivos, mandos intermedios, personal de administración, financiero, técnico, comercial, para capacitar a toda la organización en la prevención de ciberataques, robos de información, estafas online, sanciones regulatorias y el cuidado de la identidad y bienestar digital.

Crear Cultura de Ciberseguridad es la inversión más eficaz para conseguir que la organización aproveche la digitalización, sin embargo, la falta de liderazgo o no tener a alguien delegado e inclusive el poco apoyo o nulo de la alta administración dentro de una pyme se vuelve un problema que debe superarse si se desea evitar que un riesgo se materialice; al ser las personas el eslabón más débil en la cadena de ciberseguridad, el tema de cultura debe tratarse con la misma importancia para que el negocio no se vea afectado.

La falta de formación del personal es la causa de la mayor parte de las brechas en la seguridad de los datos en empresas.

Ciberataques como Ransomware, DDoS, phishing, vishing, ingeniería social, etc., son las técnicas más utilizadas por los ciberdelincuentes para realizar secuestros de dispositivos, estafas online y robos de información confidencial.

No existe autenticación, antivirus o firewall que funcione ante errores humanos.

Los objetivos de la cultura de ciberseguridad deben ser estratégicos, alineados con los objetivos de la organización y también alineados con la gestión de los riesgos que puedan afectar la consecución de estos objetivos. En este contexto, es necesario comprender cómo es la cultura de ciberseguridad actual

dentro de la organización. Pero para conocerla, primero se debe explorarla, analizar su propósito y valores compartidos, y la forma en que impacta el compromiso de las personas en el riesgo cibernético.

Asegurar el éxito de estas iniciativas constituye el apoyo del liderazgo. Por este motivo, es importante priorizar el papel que juegan los líderes al dar el ejemplo e inspirar a las personas en las buenas prácticas empresariales. Cuando asumen el compromiso activamente defendiendo la conciencia de la ciberseguridad, las personas los siguen, emulando sus principios. Por el contrario, cuando el discurso de la alta dirección no está alineado, las campañas de concientización no harán eco en el personal destino.

Presupuesto

En el caso de las pymes, es fundamental mantener los equipos tecnológicos en correcto funcionamiento y a salvo de las amenazas cibernéticas como los ransomware, malware, phishing, entre otros. Toda empresa, ya sea una gran corporación o una pyme, desea contar con una sólida ciberseguridad para defender su estructura informática de posibles ciber atacantes y aprovechar al máximo todos los recursos tecnológicos que tienen a disposición.

Ahora más que nunca la ciberseguridad está ganando terreno en las tecnologías cloud y ya no hay marcha atrás, ya que el futuro de las empresas no es regresar a la presencialidad plena. Frente a este panorama, es indispensable un mayor asesoramiento de una pyme en relación con la ciberseguridad, a fin de contar con herramientas necesarias para evitar los ataques cibernéticos.

A medida que una pyme crece en número de colaboradores y de carga de trabajo, del mismo modo crecerá en volumen de información. Es por esta razón que se debe de poner mucha atención en diseñar un buen sistema de ciberseguridad para proteger toda esa información de posibles amenazas cibernéticas; ya que, sin medidas de seguridad adecuadas, sería accesible para otras personas vulnerar la confidencialidad de esos datos. Bajo estas circunstancias, no es extraño que muchas pymes requieran ayuda en la implantación de métodos de ciberseguridad para preservar sus estructuras de posibles amenazas.

Entonces, la ciberseguridad no solamente debe ser una preocupación de las grandes empresas, sino también de las pymes, ya que un e-mail con phishing puede afectar tanto a una empresa con 5 colaboradores como a una de más de 5 mil. Además, no hay que subestimar el hecho de que una de cada tres filtraciones a la seguridad comienza con un ataque de phishing. De ahí que sea muy importante alejar estos riesgos antes de que se materialicen y represente un costo elevado para la pyme deshacerse de un virus informático o frenar un ciberataque.

Para una pyme con presencia digital, es crucial contar con soluciones que preserven las redes informáticas. Además, al operar los flujos de trabajo con una herramienta en la nube que le permita gestionar el negocio desde cualquier lugar con solo conectarse a internet, la seguridad tiene un valor agregado. Pero para lograr esto, se debe contar con una base de datos en un servidor confiable y realizar copias de seguridad diarias, cambiar contraseñas cada cierto tiempo, entre otras actividades que conlleva la ciberseguridad.

Hay diversos softwares en el mercado para asegurar la protección de los datos, por ejemplo, un software en la nube es seguro e incorpora muchas protecciones de seguridad, frente a las redes locales que pueden ser más vulnerables frente a ataques cibernéticos. Estas herramientas ofrecen actualizaciones automáticas, generan copias de seguridad diarias y es una opción adecuada en entornos remotos. No obstante, la tecnología en la nube no es la única herramienta disponible para mejorar la ciberseguridad, ya que en ocasiones puede ser costosa y no todas las pymes pueden invertir en ella.

Es acá donde surge el siguiente problema, el dinero, ese capital o inversión que se requiere para la implementación o adquisición de una herramienta robusta capaz de cubrir todas las necesidades o brechas del riesgo informático, ya que las pymes no cuentan con un gran presupuesto para tecnologías en la nube de ciberseguridad potentes como firewalls o antivirus, lo que lo limita a realizar acciones sencillas como cambiar claves y contraseñas, cifrar datos confidenciales y restringir el uso de la información a personas ajenas a la empresa o que no necesiten acceso a la información de la empresa para desempeñar sus funciones habituales, son solo algunas alternativas sencillas para proteger la información sin invertir recursos.

Muchas pymes y sus clientes se ven afectados por incidentes de ciberseguridad, lo que puede llevarlos a fracasar porque no cuentan con suficientes defensas tanto en términos de soluciones como de procesos de seguridad. A veces, solo teniendo en cuenta unos pocos pasos, ya se puede marcar la diferencia entre información protegida y riesgo de amenaza cibernética.

Organización

La seguridad cibernética se debe tomar tan en serio como otras funciones de misión crítica, como operaciones y finanzas, la ciberseguridad no es solo un problema de tecnología de información o solo exclusiva del área de TI, ante todo, se trata de una cuestión de personas.

Contrario a lo que pudiera suponerse, la ciberseguridad de una organización no inicia con la inversión en herramientas tecnológicas, más bien debe arrancar por crear desde la alta administración una cultura de prevención y prudente obtención, almacenaje, uso y desecho de información en sus diferentes estados y formatos, debido a esto es importante poner a cargo a un ejecutivo (o alguien con

autoridad): Es importante que una persona designada encabece los esfuerzos cibernéticos de su empresa. Asignar a una persona para que sea el líder de este tema resalta el compromiso con la seguridad cibernética y proporciona una experiencia profesional adicional y relevante para todos. El líder o cyber líder puede adoptar y compartir las mejores prácticas que los empleados pueden implementar y ser la persona de contacto cuando los empleados tienen preguntas o cuando ocurren incidentes cibernéticos.

Como se mencionó anteriormente, el líder o la persona designada debe crear o fomentar una cultura de conciencia cibernética: Esto significa que todos los empleados saben que juegan un papel fundamental en la resiliencia cibernética de una empresa. Este tipo de cultura se puede facilitar mediante la educación y la formación. El líder debe considerar publicar las políticas de ciberseguridad de su empresa en un lugar visible para recordar a los empleados qué hacer y que todos tienen la responsabilidad de la seguridad de la información dentro de la organización. Además, el líder debe recordar, que la cultura se crea cuando los empleados tienen un comportamiento común y que les ayudara a responder de una mejor manera la materialización de un evento que ponga en riesgo la información de la organización.

La cultura o conciencia en ciberseguridad se construye mediante comunicaciones breves y frecuentes, Por ejemplo, los boletines informativos semanales, los correos electrónicos regulares, los carteles o los protectores de pantalla pueden ser vitales para mantener a los empleados al tanto de los peligros de las infracciones cibernéticas y cómo prevenirlas. El líder debe identificar lo que es relevante para el negocio y adaptar las comunicaciones en consecuencia. Alguna sugerencia puede ser elegir un tema cibernético del mes en el que enfocarse, por ejemplo, reconocer los intentos de phishing o usar contraseñas seguras e informar de ellos a los empleados.

Otra de las tareas del líder debe ser, realizar listados de datos y sistemas que para el negocio son más importantes y críticos, de los cuales se debe priorizar y brindar mayor seguridad. Como parte de la evaluación de riesgos, se debe pensar en lo que sucedería si perdiéramos datos importantes o si el sistema fallara. Esta preparación ayudará a priorizar qué proteger. Toda organización, por pequeña que sea, debe identificar su información más sensible y asegurarse de crear copias de seguridad de esos datos, así como planificar la periodicidad con la que se deben realizar estas evaluaciones.

El líder debe desarrollar y probar un plan de respuesta a incidentes cibernéticos, tener un plan de respuesta a incidentes para dirigir sus acciones si ocurre una violación cibernética es vital. El plan de respuesta a incidentes debe cubrir la preparación en caso de un incidente, la respuesta y la rápida recuperación, es especialmente importante tener un plan de recuperación que se comunique adecuadamente a todos los empleados. Además, la realización de ejercicios o simulacros que prueben

el plan de respuesta a incidentes ayudará a los empleados a identificar sus responsabilidades durante los incidentes y les permitirá actuar de manera eficaz y segura si se producen ataques cibernéticos. La parte más importante de la preparación es tener copias de seguridad actuales que se hayan probado, especialmente para los datos más importantes.

Como podemos observar la persona designada para esta actividad se enfoca solamente en el ámbito de la ciberseguridad, lo que le demanda mucho tiempo, es acá donde surge la tercera problemática, las pymes en la mayoría de los casos o en su totalidad, no cuentan con divisiones en las áreas informáticas, mucho menos un equipo para cada una de ellas, el personal dedicado al área de TI está limitado a pocas personas, las cuales deben cubrir las necesidades que el área conlleva como por ejemplo: mantenimiento de la red, atención al usuario final, mantenimiento de servidores, control de acceso, desarrollo y pruebas, etc. Lo que los limita a enfocarse en el tema de ciberseguridad, ya que como se mencionó anteriormente entre las actividades que la persona designada debe desarrollar están: crear y fomentar la cultura de ciberseguridad, transmitir y comunicar los temas desarrollados, evaluar riesgos e identificar los datos más importantes del negocio, desarrollar y probar planes de contingencia.

Todas estas tareas del líder de la gestión de riesgo de seguridad y ciberseguridad se vuelven cada vez más complejas, por lo que es necesario que este líder se apoye en buenas prácticas reconocidas por la industria, las que le permitan organizar mejor las tareas y capitalizar experiencias de otras organizaciones.

Una de las principales mejores prácticas disponibles son los Controles de Seguridad Críticos-CIS

Los Controles de Seguridad Críticos (CIS por sus siglas en inglés) son un conjunto de controles y buenas prácticas que buscan fortalecer la postura de ciberseguridad que permitan mitigar los ataques cibernéticos más frecuentes contra sistemas y redes. Están referenciados por múltiples marcos legales regulatorios y políticas. CIS ha ido mejorando con el paso del tiempo a fin de mantenerse actualizado con los sistemas y software de vanguardia. Tomando en cuenta la migración de información y procesos en la nube, la virtualización, la movilidad, la subcontratación de profesionales, el trabajo remoto y la actualización de tácticas de los atacantes, hacen necesario respaldar la seguridad de una empresa sin importar su tamaño o giro, esto a medida que avanza hacia entornos híbridos; ya que, no puede permitirse adoptar un enfoque pasivo frente a este tipo de amenazas.

CIS simplificó el proceso para brindar orientación a las empresas sobre cómo organizar los activos, ayudando a establecer y mantener un inventario detallado de los mismos, esto a fin de mantener control sobre la infraestructura administrada.

Con la implementación de estos controles, las empresas dejarán de llevar controles manuales en hojas de cálculo o herramientas similares, las verificaciones y remediación de vulnerabilidades en los servidores serán no solo más eficientes sino que a la vez podremos tener más visibilidad sobre el nivel de obsolescencia en la infraestructura; ya que, no se dependerán de procesos manuales, lo que a su vez se convierte en una ventaja competitiva para el área de operaciones a la hora de solventar vulnerabilidades. Es de hacer notar que genera una mejor retroalimentación con el área de seguridad o ciberseguridad, es decir, en un proceso cíclico de mejora continua mientras el departamento de seguridad realiza el escaneo de vulnerabilidades y este es enviado al departamento de operaciones conteniendo la clasificación de vulnerabilidades, exposición a la que están expuestos los servidores Common Vulnerabilities Exposures (CVE). Posterior a la recepción, el departamento de operaciones evaluará los controles que aplicar para llevar a cabo la remediación de vulnerabilidades, y luego de finalizada la aplicación en los servidores Windows, solicitará nuevamente al área de seguridad realizar un nuevo escaneo con el fin de obtener un detalle de vulnerabilidades resueltas y conocer el nivel de exposición de la infraestructura.

¿Cómo pueden administrar las MiPymes sus riesgos de vulnerabilidades en infraestructura de una forma eficiente, practica y bajo estándar?

Antecedentes de (CIS)

Los Controles de Seguridad Críticos de CIS (Controles de CIS) son un conjunto prescriptivo, priorizado y simplificado de mejores prácticas de ciberseguridad que, cuando se implementan, proporcionan un programa de ciberseguridad efectivo.

Estos tratan de ayudar a las organizaciones a dar los primeros pasos en el mundo de la ciberseguridad. En mayo de 2021 CIS actualizo estos, liberando la versión v8.

Dicha versión cuenta con 18 controles de seguridad críticos, estos se encuentran organizados en tres grupos de implementación (IG1, IG2, IG3), dependiendo el tamaño de la organización y su experiencia en ciberseguridad se puede optar por empezar por uno de estos grupos.

- IG1 – Organizaciones con recursos y poca o nula experiencia en ciberseguridad
- IG2 – Empresas que emplean a personal exclusivamente para administrar y proteger la infraestructura tecnológica
- IG3 – Empresas que emplean personal especializado en ciberseguridad

CIS se encarga de monitorear en tiempo real los ciberataques (no potenciales) que ocurren a nivel mundial, para, a partir de su análisis, generar conocimiento y experiencia que ayude a los profesionales

de la ciberseguridad a proteger mejor a sus organizaciones. Básicamente, consiguen generar algo positivo de una situación negativa, convirtiéndola en conocimiento.

Los controles son parte de ese conocimiento, y establecen una serie de "controles" o "cosas que deberíamos hacer" para conseguir que nuestra infraestructura sea un poco más segura. No se meten tanto en el "cómo", pero sí establecen un "qué" bastante claro. No quiere decir que haya que hacerlo todo al pie de la letra, ni tampoco exactamente en ese orden, pero sí plantean una hoja de ruta muy razonable.

Los Grupos de Implementación (IG) son la guía recomendada para priorizar la implementación de los Controles de seguridad Críticos (CIS).

Imagen 1. Cómo Empezar

(Fuente: https://learn.cisecurity.org/cis-controls)

Grupo de implementación 1 (IG1)

Representa un estándar mínimo emergente de seguridad de la información para todas las empresas. IG1 es la vía de acceso a los controles y consta de un conjunto fundamental de 56 medidas de ciberdefensa. Las medidas de seguridad incluidas en IG1 son las que toda empresa debe aplicar para defenderse de los ataques más comunes.

En la mayoría de los casos, una empresa IG1 suele ser de tamaño pequeño a mediano con experiencia limitada en TI y ciberseguridad para dedicarse a proteger los activos y el personal de TI. Una preocupación común de estas empresas es mantener el negocio operativo, ya que tienen una tolerancia limitada al tiempo de inactividad.

La sensibilidad de los datos que están tratando de proteger es baja y principalmente rodea la información financiera y de los empleados. Las medidas seleccionadas para IG1 deben poder implementarse con experiencia limitada en seguridad cibernética y estar destinadas a frustrar ataques generales no dirigidos. Estas medidas de seguridad también se diseñarán normalmente para trabajar en conjunto con hardware y software comercial listo para usar (COTS, por sus siglas en inglés) para pequeñas empresas.

Grupo de implementación 2 (IG2)

IG2 se compone de 74 medidas adicionales y se basa en las 56 medidas identificadas en IG1.

Las 74 medidas seleccionadas para IG2 pueden ayudar a los equipos de seguridad a hacer frente a una mayor complejidad operativa. Algunas medidas de seguridad dependerán de la tecnología de nivel empresarial y la experiencia especializada para instalarlas y configurarlas correctamente.

Una empresa IG2 emplea a personas que son responsables de administrar y proteger la infraestructura de TI. Estas empresas suelen respaldar varios departamentos con diferentes perfiles de riesgo según la función y la misión del trabajo. Las unidades de pequeñas empresas pueden tener cargas de cumplimiento normativo. Las empresas IG2 a menudo almacenan y procesan información confidencial de clientes o empresas y pueden soportar breves interrupciones del servicio. Una de las principales preocupaciones es la pérdida de la confianza del público si se produce una infracción.

Grupo de implementación 3 (IG3)

IG3 se compone de 23 medidas adicionales. Se basa en las medidas de seguridad identificadas en IG1 (56) e IG2 (74) que suman las 153 medidas de seguridad en CIS.

Una empresa IG3 suele emplear expertos en seguridad que se especializan en las diferentes facetas de la ciberseguridad (p. ej., gestión de riesgos, pruebas de penetración, seguridad de aplicaciones). Los activos y datos de IG3 contienen información o funciones confidenciales que están sujetas a supervisión normativa y de cumplimiento. Una empresa IG3 debe abordar la disponibilidad de los servicios y la confidencialidad e integridad de los datos confidenciales. Los ataques exitosos pueden causar un daño significativo al bienestar público.

Las medidas de seguridad seleccionadas para IG3 deben reducir los ataques dirigidos de un adversario sofisticado y reducir el impacto de los ataques de día cero.

Por ejemplo, como se puede observar en la Tabla 1, en el control uno de CIS sus subcontroles se encuentra clasificados en los grupos de implementación en los que se deben aplicar, en este caso, los subcontroles 1.1 y 1.2 deben ser implementados en todos los grupos, mientras tanto, el 1.5 solamente si se selecciona el grupo de implementación tres.

Tabla 1. Ejemplo clasificación control uno de norma CIS versión 8

Control CIS	Sub control CIS	Título	IG1	IG2	IG3
1		Inventario y control de activos empresariales	x	x	x
1	1.1	Establecer y mantener un inventario detallado de activos empresariales	x	x	x
1	1.2	Abordar activos no autorizados		x	x
1	1.3	Utilizar una herramienta de detección activa		x	x

1	1.4	Usar el registro del Protocolo de configuración dinámica de host (DHCP), para actualizar el inventario de activos empresariales	x	x
1	1.5	Usar una herramienta de descubrimiento pasivo de activos		x

Fuente: cisecurity.org

A continuación, mostramos el listado de controles recomendados por CIS:

Tabla 2. Controles CIS

CIS Control	Nombre	Descripción
1	*Inventario y control de activos empresariales*	Establecer y mantener un inventario preciso, detallado y actualizado de todos los activos de la empresa con el potencial de almacenar o procesar datos
2	*Inventario y control de activos de software*	Establecer y mantener un inventario detallado de todo el software con licencia instalado en los activos de la empresa.
3	*Protección de datos*	Establecer y mantener un proceso de gestión de datos. En el proceso, abordar la sensibilidad de los datos, el propietario de los datos, el manejo de los datos, los límites de retención de datos y los requisitos de eliminación basados en la sensibilidad y las normas de retención de la empresa

4	*Configuración segura de activos y software empresariales*	Establecer y mantener un proceso de configuración seguro para los activos de la empresa (dispositivos de usuario final, incluidos los portátiles y móviles; dispositivos no informáticos/IoT; y servidores) y el software (sistemas operativos y aplicaciones).
5	*Gestión de cuentas*	Utilice procesos y herramientas para asignar y administrar la autorización de las credenciales de las cuentas de usuario, incluidas las cuentas de administrador, así como las cuentas de servicio, para los activos y el software empresarial.
6	*Gestión de control de acceso*	Usar procesos y herramientas para crear, asignar, administrar y revocar credenciales y privilegios de acceso para cuentas de usuario, administrador y servicio para activos empresariales y software.
7	*Gestión continua de vulnerabilidades*	Desarrollar un plan para evaluar y dar seguimiento continuo a las vulnerabilidades en todos los activos dentro de la infraestructura de la empresa, con el fin de remediar y reducir la ventana de oportunidad para los atacantes. Monitorear las fuentes de la industria pública y privada en busca de nueva información sobre amenazas y vulnerabilidades

8	*Gestión de registros de auditoría*	Recopilar, alertar, revisar y conservar registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque
9	*Protecciones de correo electrónico y navegador web*	Mejorar la protección y detección de amenazas del correo electrónico y vectores web, ya que estas son oportunidades para que los atacantes manipulen el comportamiento humano a través de su compromiso.
10	*Defensas contra malware*	Prevenir o controlar la instalación, propagación y ejecución de aplicaciones, códigos o scripts maliciosos en activos empresariales.
11	*Recuperación de datos*	Establecer y mantener prácticas de recuperación de datos suficientes para restaurar los activos empresariales incluidos en el alcance a un estado de confianza previa al incidente.
12	*Gestión de infraestructura de red*	Establecer, implementar y administrar activamente (rastrear, informar, corregir) dispositivos de red, con el fin de evitar que los atacantes exploten los servicios de red y los puntos de acceso vulnerables
13	*Supervisión y defensa de la red*	Operar procesos y herramientas para establecer y mantener la supervisión y defensas integrales de la red contra las amenazas de seguridad en toda la infraestructura de red y la base de usuarios de la empresa.

14	*Concienciación sobre seguridad y capacitación en habilidades*	Establecer y mantener un programa de concientización sobre seguridad para influir en el comportamiento de la fuerza laboral para que sea consciente de la seguridad y esté debidamente capacitado para reducir los riesgos de ciberseguridad para la empresa.
15	*Gestión de proveedores de servicios*	Desarrollar un proceso para evaluar a los proveedores de servicios que poseen datos confidenciales o que son responsables de las plataformas o procesos de TI críticos de una empresa, para garantizar que estos proveedores protejan esas plataformas y datos de manera adecuada.
16	*Seguridad del software de aplicación*	Administrar el ciclo de vida de seguridad del software desarrollado, alojado o adquirido internamente para prevenir, detectar y corregir las debilidades de seguridad antes de que puedan afectar a la empresa.
17	*Gestión de respuesta a incidentes*	Establecer un programa para desarrollar y mantener una capacidad de respuesta a incidentes (por ejemplo, políticas, planes, procedimientos, roles definidos, capacitación y comunicaciones) para preparar, detectar y responder rápidamente a un ataque.

18	*Pruebas de penetración*	Pruebe la eficacia y la resistencia de los activos empresariales mediante la identificación y explotación de debilidades en los controles (personas, procesos y tecnología) y la simulación de los objetivos y acciones de un atacante.

A continuación, se detallan los sub- controles de cada uno de los controles CIS:

CIS Control 1:

Resumen:

Gestione activamente (inventario, seguimiento y corrección) todos los activos de la empresa (dispositivos de usuarios finales, incluidos equipos portátiles y teléfonos móviles; dispositivos de red; Dispositivos no informáticos/Internet de las Cosas (IoT); y servidores) conectados a la infraestructura física, virtualmente, remotamente, y aquellos del ambiente de la nube, para conocer con precisión la totalidad de los activos que necesitan ser monitoreados y protegidos dentro de la empresa. Esto también apoyará la identificación de activos no autorizados y no administrados para eliminar o remediar.

- 1.1: Establecer y mantener un inventario detallado de los activos de la empresa
- 1.2: Tratar los activos no autorizados
- 1.3: Utilizar una herramienta de detección activa
- 1.4: Utilizar el registro del protocolo de configuración dinámica de host (DHCP) para actualizar el inventario de activos de la empresa
- 1.5: Utilizar una herramienta de descubrimiento pasivo de activos

CIS Control 2:

Resumen:

Gestione activamente (inventario, seguimiento y corrección) todo el software (sistemas operativos y aplicaciones) dentro de la red. Únicamente el software autorizado debe ser instalado y ejecutado, y aquellos software no autorizados ni gestionados que se encuentren se impida la instalación y/o ejecución.

- 2.1: Establecer y mantener un inventario de software
- 2.2: Asegúrese de que el software autorizado es actualmente compatible
- 2.3: Abordar el software no autorizado
- 2.4: Utilizar herramientas automatizadas de inventario de software
- 2.5: Software autorizado por lista de aplicaciones permitidas

- 2.6: Lista permitida de bibliotecas autorizadas
- 2.7: Lista de scripts autorizados

CIS Control 3:

Resumen:

Desarrollar procesos y controles técnicos para identificar, clasificar, manejar, retener y eliminar de forma segura los datos.

- 3.1: Establecer y mantener un proceso de gestión de datos
- 3.2: Establecer y mantener un inventario de datos
- 3.3: Configurar listas de control de acceso a los datos
- 3.4: Hacer cumplir la retención de datos
- 3.5: Eliminar los datos de forma segura
- 3.6: Cifrar los datos en los dispositivos de los usuarios finales
- 3.7: Establecer y mantener un esquema de clasificación de datos
- 3.8: Documentar los flujos de datos
- 3.9: Cifrar los datos en medios extraíbles
- 3.10: Cifrar datos sensibles en tránsito
- 3.11: Cifrar los datos sensibles en reposo
- 3.12: Segmentar el procesamiento y el almacenamiento de datos en función de su sensibilidad
- 3.13: Implantar una solución de prevención de pérdida de datos
- 3.14: Registrar el acceso a datos sensibles

CIS Control 4:

Resumen:

Establecer y mantener la configuración segura de los activos empresariales (Dispositivos de usuarios, incluidos portátiles y móviles; dispositivos de red; dispositivos no informáticos/IoT; y servidores) y software (Sistemas operativos y aplicaciones).

- 4.1 Establecer y mantener un proceso de configuración seguro
- 4.2 Establecer y mantener un proceso de configuración seguro para la infraestructura de red
- 4.3 Configurar el bloqueo automático de la sesión en los activos de la empresa
- 4.4 Implementar y gestionar un firewall en los servidores
- 4.5 Implementar y gestionar un firewall en dispositivos de usuario final
- 4.6 Gestionar de forma segura los activos y el software de la empresa
- 4.7 Gestionar las cuentas por defecto en los activos y el software de la empresa
- 4.8 Desinstalar o desactivar servicios innecesarios en los activos y software de la empresa
- 4.9 Configurar servidores DNS de confianza en activos empresariales
- 4.10 Aplicar el bloqueo automático de dispositivos en los dispositivos portátiles de los usuarios finales
- 4.11 Reforzar la capacidad de borrado remoto en dispositivos portátiles de usuario final

- 4.12 Separar los espacios de trabajo de la empresa en los dispositivos móviles de los usuarios finales

CIS Control 5:

Resumen:

Utilice procesos y herramientas para asignar y administrar la autorización de las credenciales de las cuentas de usuario, incluidas las cuentas de administrador, así como las cuentas de servicio, para los activos y el software empresarial.

- 5.1: Establecer y mantener un inventario de cuentas
- 5.2: Utilice contraseñas únicas
- 5.3: Deshabilitar cuentas inactivas
- 5.4: Restringir privilegios de administrador a cuentas de administrador dedicadas
- 5.5: Establecer y mantener un inventario de cuentas de servicio
- 5.6: Centralizar la gestión de cuentas

CIS Control 6:

Resumen:

Usar procesos y herramientas para crear, asignar, administrar y revocar credenciales y privilegios de acceso para cuentas de usuario, administrador y servicio para activos empresariales y software.

- 6.1: Establecer un proceso para conceder accesos
- 6.2: Establecer un proceso de revocación de acceso
- 6.3: Exigir MFA para aplicaciones expuestas externamente
- 6.4: Exigir MFA para el acceso remoto a la red
- 6.5: Exigir MFA para el acceso administrativo
- 6.6: Establecer y mantener un inventario de sistemas de autenticación y autorización
- 6.7: Control de Acceso Centralizado
- 6.8: Definir y mantener el control de acceso basado en roles

CIS Control 7:

Resumen:

Desarrollar un plan para evaluar y dar seguimiento continuo a las vulnerabilidades en todos los activos dentro de la infraestructura de la empresa, con el fin de remediar y reducir la ventana de oportunidad para los atacantes. Monitorear las fuentes de la industria pública y privada en busca de nueva información sobre amenazas y vulnerabilidades.

- 7.1: Establecer y mantener un proceso de gestión de vulnerabilidades
- 7.2: Establecer y mantener un proceso de remediación
- 7.3: Realice una gestión automatizada de parches del sistema operativo
- 7.4: Realizar la administración automatizada de parches de aplicaciones
- 7.5: Realizar análisis automatizados de vulnerabilidades de activos internos de la empresa

- 7.6: Realice análisis automatizados de vulnerabilidades de activos empresariales expuestos externamente
- 7.7: Remediar las vulnerabilidades detectadas

CIS Control 8:

Resumen:

Recopilar, alertar, revisar y conservar registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.

- 8.1: Establecer y mantener un proceso de gestión de registros de auditoría
- 8.2: Recopilar registros de auditoría
- 8.3: Garantizar un almacenamiento adecuado del registro de auditoría
- 8.4: Estandarizar la sincronización de hora
- 8.5: Recopilar registros de auditoría detallados
- 8.6: Recopilar registros de auditoría de consultas de DNS
- 8.7: Recopilar registros de auditoría de solicitudes de URL
- 8.8: Recopilar registros de auditoría de la línea de comandos
- 8.9: Centralice Audit Logs
- 8.10: Conservar registros de auditoría
- 8.11: Realizar revisiones de registros de auditoría
- 8.12: Recopilar registros de auditorías para proveedores de servicios

CIS Control 9:

Resumen:

Mejorar la protección y detección de amenazas del correo electrónico y vectores web, ya que estas son oportunidades para que los atacantes manipulen el comportamiento humano a través de su compromiso.

- 9.1: Garantizar el uso de solo navegadores y clientes de correo electrónico totalmente compatibles
- 9.2: Usar servicios de filtrado DNS
- 9.3: Mantener y aplicar filtros de URL basados en la red
- 9.4: Restringir extensiones innecesarias o no autorizadas de navegador y cliente de correo electrónico
- 9.5: Implementar DMARC
- 9.6: Bloquear tipos de archivos innecesarios
- 9.7: Implementar y mantener protecciones antimalware del servidor de correo electrónico

CIS Control 10:

Resumen:

Prevenir o controlar la instalación, propagación y ejecución de aplicaciones, códigos o scripts maliciosos en activos empresariales.

- 10.1: Implementar y mantener software antimalware
- 10.2: Configurar actualizaciones automáticas de firmas de Antimalware
- 10.3: Deshabilitar la ejecución y la reproducción automática para medios extraíbles
- 10.4: Configurar el análisis antimalware automático de medios extraíbles
- 10.5: Habilitar funciones anti-explotación
- 10.6: Administrar de forma centralizada el software antimalware
- 10.7: Utilice el software antimalware basado en el comportamiento

CIS Control 11:

Resumen:

Establecer y mantener prácticas de recuperación de datos suficientes para restaurar los activos empresariales incluidos en el alcance a un estado de confianza previo al incidente.

- 11.1: Establecer y mantener un proceso de recuperación de datos
- 11.2: Realice copias de seguridad automatizadas
- 11.3: Proteja los datos de recuperación
- 11.4: Establecer y mantener una instancia aislada de datos de recuperación
- 11.5: Prueba de recuperación de datos

CIS Control 12:

Resumen:

Establecer, implementar y administrar activamente (rastrear, informar, corregir) dispositivos de red, con el fin de evitar que los atacantes exploten los servicios de red y los puntos de acceso vulnerables.

- 12.1: Asegúrese de que la infraestructura de red esté actualizada
- 12.2: Establecer y mantener una arquitectura de red segura
- 12.3: Gestione de forma segura la infraestructura de red
- 12.4: Establecer y mantener diagramas de arquitectura
- 12.5: Centralice la autenticación, la autorización, y la auditoría de la red (AAA)
- 12.6: Uso de protocolos seguros de administración de redes y comunicaciones
- 12.7: Asegúrese de que los dispositivos remotos utilicen una VPN y se conecten a la infraestructura AAA de una empresa
- 12.8: Establecer y mantener recursos informáticos dedicados para todo el trabajo administrativo

CIS Control 13:

Resumen:

Operar procesos y herramientas para establecer y mantener la supervisión y defensa integrales de la red contra las amenazas de seguridad en toda la infraestructura de red y la base de usuarios de la empresa.

- 13.1: Centralizar alertas de eventos de seguridad
- 13.2: Implemente una solución de detección de intrusiones basada en host
- 13.3: Implementación de una solución de detección de intrusiones en la red
- 13.4: Realizar filtrado de tráfico entre segmentos de red
- 13.5: Gestionar el control de acceso para activos remotos
- 13.6: Recopilar registros de flujo de tráfico de red
- 13.7: Implementar una solución de prevención de intrusiones basada en host
- 13.8: Implementar una solución de prevención de intrusiones en la red
- 13.9: Implementar el control de acceso a nivel de puerto
- 13.10: Realizar el filtrado en la capa de aplicación
- 13.11: Ajustar los umbrales de alerta de eventos de seguridad

CIS Control 14:

Resumen:

Establecer y mantener un programa de concientización sobre seguridad para influir en el comportamiento de la fuerza laboral para que sea consciente de la seguridad y esté debidamente capacitado para reducir los riesgos de ciberseguridad para la empresa.

- 14.1: Establecer y mantener un programa de concientización sobre seguridad
- 14.2: Capacitar a los miembros de la plana laboral para que reconozcan los ataques de ingeniería social
- 14.3: Capacitar a los miembros de la plana laboral sobre las mejores prácticas de autenticación
- 14.4: Capacitar a la fuerza laboral en las mejores prácticas de manejo de datos
- 14.5: Capacitar a los miembros de la plana laboral sobre las causas de la exposición involuntaria de datos
- 14.6: Capacitar a los miembros de la plana laboral sobre el reconocimiento y la notificación de incidentes de seguridad
- 14.7: Capacitar al personal sobre cómo identificar e informar si sus activos empresariales carecen de actualizaciones de seguridad
- 14.8: Capacitar a la plana laboral sobre los peligros de conectarse y transmitir datos empresariales a través de redes inseguras
- 14.9: Llevar a cabo capacitación en habilidades y concientización sobre seguridad para roles específicos

CIS Control 15:

Resumen:

Desarrollar un proceso para evaluar a los proveedores de servicios que poseen datos confidenciales o que son responsables de las plataformas o procesos de TI críticos de una empresa, para garantizar que estos proveedores protejan esas plataformas y datos de manera adecuada.

- 15.1: Establecer y mantener un inventario de proveedores de servicios
- 15.2: Establecer y mantener una política de gestión de proveedores de servicios
- 15.3: Clasificar proveedores de servicios
- 15.4: Asegúrese de que los contratos de los proveedores de servicios incluyan requisitos de seguridad
- 15.5: Evaluar proveedores de servicios
- 15.6: Supervisar proveedores de servicios
- 15.7: Dar de baja de forma segura a los proveedores de servicios

CIS Control 16:

Resumen:

Administrar el ciclo de vida de seguridad del software desarrollado, alojado o adquirido internamente para prevenir, detectar y corregir las debilidades de seguridad antes de que puedan afectar a la empresa.

- 16.1: Establecer y mantener un proceso de desarrollo de aplicaciones seguro
- 16.2: Establecer y mantener un proceso para aceptar y abordar las vulnerabilidades del software
- 16.3: Realice un análisis de la causa raíz de las vulnerabilidades de seguridad
- 16.4: Establecer y administrar un inventario de componentes de software de terceros
- 16.5: Utilice componentes de software de terceros actualizados y confiables
- 16.6: Establecer y mantener un sistema y proceso de clasificación de gravedad para las vulnerabilidades de las aplicaciones
- 16.7: Usar plantillas de configuración de protección estándar para la infraestructura de aplicaciones
- 16.8: Sistemas de producción separados y sistemas de no producción
- 16.9: Capacitar a los desarrolladores en conceptos de seguridad de aplicaciones y codificación segura
- 16.10: Aplicar principios de diseño seguro en arquitecturas de aplicaciones
- 16.11: Aprovechar los módulos o servicios examinados para los componentes de seguridad de las aplicaciones
- 16.12: Implementar verificaciones de seguridad a nivel de código
- 16.13: Realizar pruebas de penetración de aplicaciones
- 16.14: Realizar modelado de amenazas

CIS Control 17:

Resumen:

Establecer un programa para desarrollar y mantener una capacidad de respuesta a incidentes (por ejemplo, políticas, planes, procedimientos, roles definidos, capacitación y comunicaciones) para preparar, detectar y responder rápidamente a un ataque.

- 17.1 Designar personal para administrar el manejo de incidentes
- 17.2 Establecer y mantener información de contacto para informar incidentes de seguridad
- 17.3 Establecer y mantener un proceso empresarial para informar de incidentes
- 17.4 Establecer y mantener un proceso de respuesta a incidentes
- 17.5 Asignar Roles Claves y Responsabilidades
- 17.6 Definir mecanismos de comunicación durante la respuesta a incidentes
- 17.7 Realizar ejercicios rutinarios de respuesta a incidentes
- 17.8 Realizar revisiones posteriores a un incidente
- 17.9 Establecer y mantener umbrales de incidentes de seguridad

CIS Control 18:

Resumen:

Pruebe la eficacia y la resistencia de los activos empresariales mediante la identificación y explotación de debilidades en los controles (personas, procesos y tecnología) y la simulación de los objetivos y acciones de un atacante.

- 18.1 Establecer y mantener un programa de pruebas de penetración
- 18.2 Realizar pruebas periódicas de penetración externa
- 18.3 Corregir los resultados de la prueba de penetración
- 18.4 Valide las medidas de seguridad
- 18.5 Realice pruebas periódicas de penetración interna

Problemática actual de las pymes

El objetivo de esta investigación es plantear un proceso práctico y sencillo de implementar para proteger los activos de información de las PYME categorizando y remediando las vulnerabilidades a las que están expuestos los servidores de la empresa.

Los ataques cibernéticos no solo son sufridos exclusivamente de las grandes empresas, para los atacantes es más fácil atacar 50 PYMES con una baja seguridad informática y lograr su objetivo, que atacar una multinacional con seguridad robusta y que probablemente le demandara más tiempo e ingenio para lograr su cometido o inclusive no lo logre.

Los procesos manuales es el enfoque en esta investigación ya que el esperado es que la PYME no realiza sus escaneos de forma automática o utilizando la herramienta adecuada, sino que utilizan un listado (checklist) en donde van colocando si cumple o no cumple con la seguridad, esta forma de hacer el proceso les impide conocer realmente el nivel de riesgo a la que están expuestos, ya que no existe un criterio, ni mucho menos una escala que les ayude a categorizar el riesgo para su correcto

tratamiento y remediación, dejándolos desprotegidos ante cualquier ataque que sea dirigido a la empresa.

Problemática nivel regional y estudios

Las pymes juegan un papel muy importante en la económica de un país, ellas contribuyen al PIB de cada país, generan empleo, aportan en el desarrollo de la economía en un país, etc.

Los principales estudios realizados sobre las tendencias actuales, tanto en modelos teóricos como empíricos, hechos por destacados especialistas en el campo de la administración y dirección de empresas en los últimos 20 años han sido focalizados en los negocios de gran dimensión, olvidando en gran medida a las pequeñas y medianas empresas (Pymes).

A pesar de los escasos estudios en las empresas de menor magnitud, las Pymes siguen contribuyendo a la economía (generación de empleos y producción de riqueza) en la mayoría de las regiones de diferentes países. Por ello la importancia de desarrollar estudios que contemplen el comportamiento de estas variables en el campo de las MiPymes. (fuente - La gestión del conocimiento y las TIC, su efecto en la innovación y el rendimiento de las pymes / Luis Enrique Valdez Juárez - 2017 url: https://dialnet.unirioja.es/servlet/tesis?codigo=172547)

Las pymes representan actores claves para incrementar el crecimiento potencial de América Latina. Estas empresas se caracterizan por una gran heterogeneidad en su acceso a mercados, tecnologías y capital humano, así como su vinculación con otras empresas, factores que afectan su productividad, capacidad de exportación y potencial de crecimiento. (fuente - Acerca de Microempresas y Pymes

Url: https://www.cepal.org/es/temas/pymes/acerca-microempresas-pymes)

Por un lado, constituyen un componente fundamental del entramado productivo en la región: representan alrededor de 99% del total de empresas y dan empleo a cerca de 67% del total de trabajadores. Por otro lado, su contribución al PIB es relativamente baja, lo que revela deficiencias en los niveles de productividad de estas. Por ejemplo, las empresas grandes en la región tienen niveles de productividad hasta 33 veces la productividad de las microempresas y hasta seis para las pequeñas, mientras que en los países OCDE estas cifras oscilan entre un 1.3 y 2.4 veces. (fuente - Acerca de Microempresas y Pymes

Url:https://www.cepal.org/es/temas/pymes/acerca-microempresas-pymeshttps://www.cepal.org/es/temas/pymes/acerca-microempresas-pymes)

Las MiPymes no pueden quedar al margen de este proceso. Más aún, su peso en el tejido productivo (el 99% de las empresas formales latinoamericanas son pymes) y en el empleo (el 61% del empleo formal es generado por empresas de ese tamaño) las vuelve un actor central para garantizar la viabilidad y eficacia de la transformación generadora de una nueva dinámica de desarrollo que permita un crecimiento económico más rápido y continuo, que al mismo tiempo sea incluyente y sostenible. (fuente - M. Dini y G. Stumpo (coords.), "MiPymes en América Latina: un frágil desempeño y nuevos desafíos para las políticas de fomento", Documentos de Proyectos (LC/TS.2018/75/ Rev.1), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2020.)

Las pymes son un componente fundamental del tejido empresarial en América Latina, lo que se manifiesta en varias dimensiones, como su participación en el número total de empresas o la creación de empleo. Ello se contrapone a una participación en el producto interno bruto (PIB) regional de tan solo el 25%, situación que contrasta con la de los países de la Unión Europea, donde esta cifra alcanza, en promedio, el 56%. (fuente - M. Dini y G. Stumpo (coords.), "MiPymes en América Latina: un frágil desempeño y nuevos desafíos para las políticas de fomento", Documentos de Proyectos (LC/TS.2018/75/ Rev.1), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2020.)

Un aspecto fundamental de las pymes latinoamericanas es su heterogeneidad. En primer lugar, encontramos microempresas cuya gestación suele responder a necesidades individuales de autoempleo y que a menudo se encuentran en una situación de informalidad, que incluye bajos niveles de capital humano, dificultad para acceder a recursos financieros externos, escasa internacionalización y realización de actividades con bajos requerimientos técnicos.

En el otro extremo, se encuentran las pymes de alto crecimiento, que se caracterizan por tener un comportamiento mucho más dinámico, tanto respecto de la facturación como de la creación de puestos de trabajo, y cuyo desempeño responde al aprovechamiento de oportunidades de mercado a través de una gestión empresarial eficiente e innovadora. El concepto de tamaño de empresa, por tanto, oculta realidades muy diversas en este tipo de unidades productivas. (fuente - M. Dini y G. Stumpo (coords.), "MiPymes en América Latina: un frágil desempeño y nuevos desafíos para las políticas de fomento", Documentos de Proyectos (LC/TS.2018/75/ Rev.1), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2020.)

La información cuantitativa sobre las pymes de América Latina es bastante escasa y, a menudo, de mala calidad. Por esta razón es difícil analizar la evolución del desempeño de estas empresas y, a veces,

existen problemas para estimar correctamente su peso en la producción y el empleo. Esto se debe a las definiciones de pymes que se utilizan en los países de la región, pero también a la frecuencia y a los criterios empleados para recolectar la información, en la región es posible encontrar criterios basados en el personal ocupado, las ventas anuales (en ocasiones con límites distintos según el sector de actividad económica), y el valor de los activos o de las exportaciones, a veces combinados entre sí.

En algunos casos no existe una definición nacional y se utiliza la de una institución internacional. También puede ocurrir que en el mismo país coexistan varias definiciones de pymes; tradicionalmente, una basada en la cantidad de empleados y utilizada por los institutos de estadística y otra que sigue los criterios de las instituciones de fomento a las empresas, como volumen de ventas y activos. (fuente - M. Dini y G. Stumpo (coords.), "MiPymes en América Latina: un frágil desempeño y nuevos desafíos para las políticas de fomento", Documentos de Proyectos (LC/TS.2018/75/ Rev.1), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2020.)

Considerando la economía formal, las pymes representan el 99,5% de las empresas de la región y la gran mayoría son microempresas (88,4% del total). Esta distribución se ha mantenido relativamente estable a lo largo de la última década, aunque ha habido un incremento relativo de las pequeñas y medianas empresas y una ligera reducción de las microempresas. (fuente - M. Dini y G. Stumpo (coords.), "MiPymes en América Latina: un frágil desempeño y nuevos desafíos para las políticas de fomento", Documentos de Proyectos (LC/TS.2018/75/ Rev.1), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2020.)

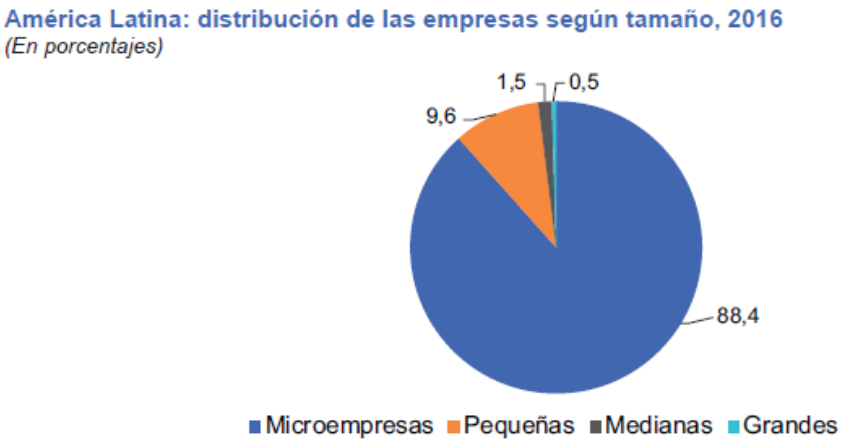


Imagen 2.Distribución de empresas según tamaño

(Fuente - M. Dini y G. Stumpo (coords.), "MiPymes en América Latina: un frágil desempeño y nuevos desafíos para las políticas de fomento", Documentos de Proyectos (LC/TS.2018/75/ Rev.1), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2020.)

América Latina: cantidad de empresas según sector de actividad y tamaño, 2016
(En porcentajes)

Sector	Microempresa	Pequeña	Mediana	Grande	Total
Agricultura, ganadería, caza, silvicultura y pesca	80	16	3	1	100
Explotación de minas y canteras	68	23	6	3	100
Industria manufacturera	82	14	3	1	100
Suministro de electricidad, gas y agua	70	20	6	4	100
Construcción	76	19	4	1	100
Comercio al por mayor y menor	92	7	1	0	100
Hoteles y restaurantes	89	10	1	0	100
Transporte, almacenamiento y comunicaciones	83	13	2	1	100
Intermediación financiera	81	14	3	2	100
Actividades inmobiliarias, empresariales y de alquiler	87	10	2	0	100
Enseñanza	76	19	4	1	100
Servicios sociales y de salud	89	9	1	0	100
Otras actividades comunitarias, sociales y personales	95	4	1	0	100
Total	88,4	9,6	1,5	0,5	100

Imagen 3. Cantidad de empresas según sector

(Fuente - M. Dini y G. Stumpo (coords.), "MiPymes en América Latina: un frágil desempeño y nuevos desafíos para las políticas de fomento", Documentos de Proyectos (LC/TS.2018/75/ Rev.1), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2020.)

La presencia de microempresas es mayoritaria en todos los sectores de la economía y en algunos casos supera el 90% del total de las empresas: por ejemplo, en el comercio y en el sector de "otras actividades comunitarias, sociales y personales". En particular, el comercio es un sector en que se concentra la mayor cantidad de microempresas formales.

Las bajas barreras a la entrada favorecen, en este caso, la proliferación de empresas de tamaño muy reducido que, a menudo, responden más a estrategias de autoempleo y sobrevivencia económica que a un verdadero proceso de desarrollo empresarial. En el comercio también está presente una cantidad importante de pymes; sin embargo, en el caso de estas empresas, la industria, en particular al tratarse de las empresas medianas, y las "actividades inmobiliarias, empresariales y de alquiler" concentran una cantidad significativa de unidades productivas. (fuente - M. Dini y G. Stumpo (coords.), "MiPymes en América Latina: un frágil desempeño y nuevos desafíos para las políticas de fomento", Documentos de Proyectos (LC/TS.2018/75/ Rev.1), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2020.)

Para entender a cabalidad estos fenómenos es necesario considerar la inserción de las pymes en la estructura productiva de los países de la región. En términos generales, puede decirse que el empleo de las microempresas se concentra sobre todo en el comercio y en algunos servicios de escaso valor agregado. En el segmento de las pequeñas empresas, los rubros más importantes son el comercio minorista, en menor medida la industria manufacturera, y, en algunos casos, la construcción. En

cambio, si se consideran las empresas medianas, la industria puede llegar a ser el sector con el porcentaje más grande de ocupados, a pesar de que el comercio sigue manteniendo un peso relativo importante, aunque en general inferior al de la industria.

En las grandes empresas, el empleo se concentra principalmente en la manufactura y en algunos servicios de mayor valor agregado.

Esta distribución del empleo presenta cierta variabilidad de acuerdo con las características específicas de la estructura productiva de cada país de la región; por ejemplo, en los países de menor desarrollo industrial, el comercio puede ser relevante en términos de empleo también para el conjunto de las grandes empresas y llegar a igualar, o hasta superar, la importancia de la industria. Igualmente, en ese mismo segmento de empresas, los servicios de telecomunicaciones e intermediación financiera pueden tener un peso mayor en aquellas economías de menor tamaño y más especializadas en los sectores mencionados. (fuente - M. Dini y G. Stumpo (coords.), "MiPymes en América Latina: un frágil desempeño y nuevos desafíos para las políticas de fomento", Documentos de Proyectos (LC/TS.2018/75/ Rev.1), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2020.)

cuáles son los retos que enfrentan las MiPymes en Latam

El desarrollo de las pymes abarca problemáticas muy heterogéneas, que van desde aspectos laborales y tributarios, a temas relacionados con el financiamiento, el desarrollo y la difusión de nuevas tecnologías, la constitución de estrategias colectivas, políticas arancelarias, de educación e investigación, inversiones en infraestructura, etc.

Cada una de estas áreas tiene a menudo especificidades sectoriales relevantes, en las cuales intervienen varios organismos reguladores y de fomento, como bancos, agencias de innovación, instituciones de promoción de las exportaciones, institutos públicos de formación, entidades ministeriales de distintas carteras (economía o industria, trabajo, relaciones exteriores y política interior), gobiernos locales y universidades. Todo esto configura un entramado complejo de entidades cuya coordinación representa uno de los grandes desafíos para el desarrollo de una política de fomento efectiva. (fuente - M. Dini y G. Stumpo (coords.), "MiPymes en América Latina: un frágil desempeño y nuevos desafíos para las políticas de fomento", Documentos de Proyectos (LC/TS.2018/75/ Rev.1), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2020.)

Los principales problemas y debilidades detectados se refieren a tres aspectos:

• La institucionalidad de fomento sigue siendo frágil en muchos países. Con pocas excepciones, no hay entidades públicas especializadas que logren desarrollar estrategias de largo plazo, y la participación

del mundo empresarial en el diseño e implementación de las políticas es aún muy esporádica e incipiente.

• Falta una visión estratégica sobre el rol de las pymes en la transformación productiva, lo que hace muy difícil la integración de las acciones de apoyo a las micro, pequeñas y medianas empresas con los programas más generales de transformación productiva. Más aún, como no quedan claras las metas y los objetivos de las políticas, a menudo no se logra garantizar la convergencia de las acciones emprendidas por las entidades que, desde perspectivas distintas, concurren a su cumplimiento.

• A pesar de los esfuerzos realizados por parte de las entidades públicas, la fragmentación de la acción de apoyo en centenares de actividades de reducido alcance limita su capacidad de producir impactos visibles.

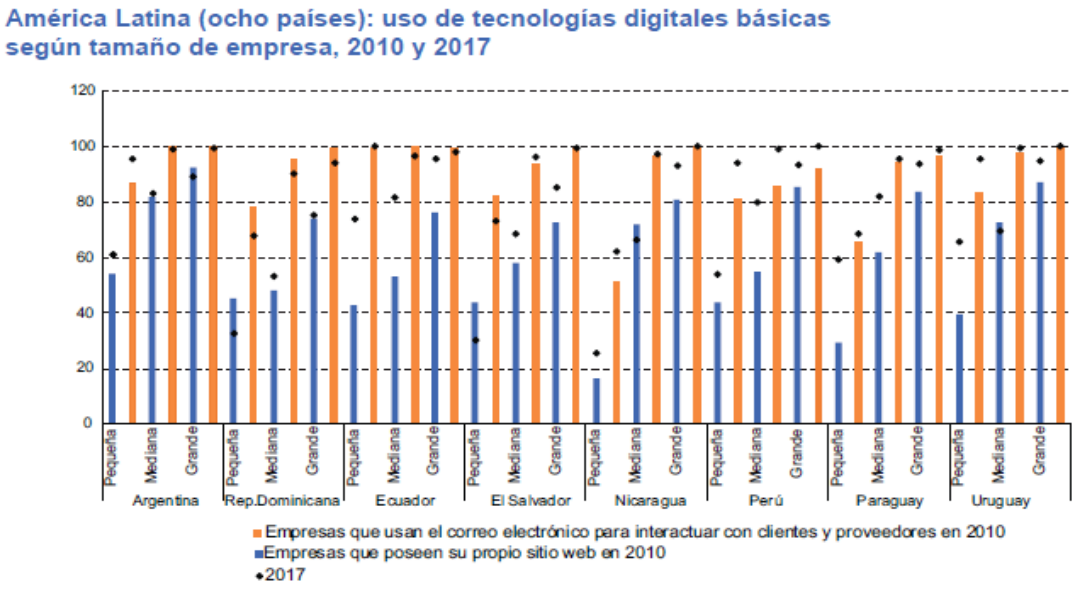


Imagen 4. Uso de tecnologías digitales según tamaño de empresas

(fuente - Base de Banco Mundial, Enterprise Surveys, base de datos en línea, http://www.enterprisesurveys.org)

Entender la génesis de estos problemas es una condición necesaria para impulsar una nueva generación de políticas de fomento que permitan a los países de la región enfrentar los desafíos en el camino hacia un nuevo estilo de desarrollo. (fuente - M. Dini y G. Stumpo (coords.), "MiPymes en América Latina: un frágil desempeño y nuevos desafíos para las políticas de fomento", Documentos de Proyectos (LC/TS.2018/75/ Rev.1), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2020.)

En este escenario, cabe preguntarse dónde se colocan las pymes y cuáles factores inciden en determinar su colocación en el proceso de transición entre los dos mundos. La falta de datos actualizados y pertinentes no permite un análisis exhaustivo del nivel alcanzado por la penetración de las tecnologías digitales en su organizaciones productivas y modelos de negocio.

Una luz parcial sobre este punto es brindada por las Encuestas Empresariales del Banco Mundial en una decena de países de América Latina que analizan la incorporación de tecnologías digitales maduras (véase el gráfico América Latina (ocho países): uso de tecnologías digitales básicas según tamaño de empresa, 2010 y 2017). En particular, el estudio compara el porcentaje de pymes y grandes empresas que tenían su propia página web y que utilizaban el correo electrónico para comunicarse con clientes y proveedores, en 2010 y 2017.

Las tendencias que destacan con claridad son, en primer lugar, que en ambas variables el grado de penetración de las tecnologías incrementa con el aumentar del tamaño de las empresas.

En segundo lugar, que la observación correspondiente a 2017 registra generalmente avances significativos en las dos variables. No obstante, también hay señales de alerta preocupantes: el uso del mail se ha masificado entre las empresas, pero no entre las pequeñas. Especialmente en países con menor grado de desarrollo, como Nicaragua y el Paraguay, las brechas con las grandes empresas aún bordean los 30-40 puntos. Por lo que concierne el uso de páginas web la distribución es mucho menos homogénea y las diferencias alcanzan valores aún más altos.

Particularmente llamativo parece ser el hecho que entre las medianas empresas (y, en algunos países, hasta entre las grandes) la penetración de esta tecnología relativamente poco sofisticada aún sea tan baja, con numerosos países entre 70% y 80%.

En cuanto al desarrollo de nuevos emprendimientos intensivos en tecnología de la información y gestión de datos, los estudios sugieren igualmente un bajo desempeño de la región en cuanto a emprendimientos digitales. Según el Global Entrepreneurship Monitor (GEM), el análisis de la actividad emprendedora en la región revela una muy frágil dinámica de las industrias digitales locales y la persistencia de modelos de negocios en sectores de baja intensidad tecnológica.

América Latina destaca por ser una de las regiones con el mayor nivel de emprendimientos tempranos en el mundo (TEA por sus siglas en ingles), con un 18,5% de la población en edad de trabajar que emprende, y ser, al mismo tiempo, una de las regiones que menos emprende en el sector de las TIC (2,8% de la tasa de emprendimiento temprano, aproximadamente la mitad de lo que registran los países más industrializados).

Los altos niveles de emprendimiento parecieran explicarse en buena medida, por el alto índice de emprendimiento por necesidad que existe en la región: en 2017, casi el 30% de los emprendedores tempranos declararon emprender por necesidad y no por oportunidad. En cuanto al débil desempeño de la región en emprendimientos digitales, las causas podrían estar relacionadas con un sistema de apoyo aún incipiente. (fuente - M. Dini y G. Stumpo (coords.), "MiPymes en América Latina: un frágil desempeño y nuevos desafíos para las políticas de fomento", Documentos de Proyectos (LC/TS.2018/75/ Rev.1), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2020.)

Desde este punto de vista, cabe destacar que las tecnologías digitales no representan simplemente una nueva área tecnológica que se suma a las muchas otras que influencian el desarrollo de las empresas. Los cambios que estas tecnologías están generando son mucho más profundos y transversales, y están alterando radicalmente la esencia misma del quehacer empresarial, las estrategias competitivas y las modalidades de aprendizaje de las empresas.

Para que las políticas de fomento se adecúen a esta transformación es preciso disponer de un marco conceptual que permita entender las modalidades específicas de esta evolución y los factores que la condicionan. Esta sección se propone dar un paso en esta dirección, esbozando algunas piezas de este marco de referencia para lo que concierne a las pymes.

En primer lugar, estas tecnologías generan tanto impactos positivos como negativos en las empresas de menor tamaño. En el lado positivo, la disminución de los precios de las tecnologías informáticas y la continua mejora de las tecnologías de comunicación seguirán siendo un factor de expansión de estas herramientas, favoreciendo una penetración cada vez más capilar, especialmente importante para las áreas que por el momento tienen escaso acceso a internet (CEPAL, 2016a y 2016b).

Estas herramientas amplían significativamente las potencialidades de negocio de las empresas y, en el caso de las empresas de menor tamaño, su impacto resulta en la reducción de los costos de acceso al mercado, la eliminación de los intermediarios, una conexión más directa con los clientes y una retroalimentación continua desde los mercados (CCI, 2016).

Otro aspecto que puede incidir en la realidad de las pymes es la posibilidad de que se bajen las barreras de entradas para la creación de empresas que contemplen modelos de negocios intensivos en tecnología de información y gestión de datos. Las tecnologías digitales generan también nuevos obstáculos para las pequeñas empresas. De prevalecer sobre los incentivos, estos podrían determinar un atraso muy importante en el proceso de incorporación de las tecnologías y la ampliación de las brechas competitivas que ya existen con las empresas más grandes.

El primer obstáculo concierne las economías de escala asociadas con la incorporación de la digitalización del conjunto de funciones productivas, administrativas y comerciales de las empresas. Si bien ha habido una disminución relevante de los costos de los aparatos (hardware), en paralelo se ha incrementado significativamente la complejidad de los sistemas necesarios para integrar la gestión productiva. La complejidad de dichos sistemas genera dos barreras importantes: la primera es de carácter financiero, pues la reorganización de toda la estructura de gestión y producción puede requerir de una renovación significativa de maquinarias, inversiones en nuevos sistemas de control y calidad, transformaciones importantes de layout y logística, etc.

La segunda, posiblemente aún más significativa, es de tipo estratégico y concierne la capacidad de las empresas de entender las posibilidades que las nuevas tecnologías les ofrecen para reinventar su modelo de negocio, ajustar sus sistemas de gestión, reorganizar su estructura productiva, etc. Los límites que padecen las empresas pequeñas en estos frentes son múltiples y van desde la escasa profesionalización en temas de gestión, hasta la falta de contacto con entidades (como los centros tecnológicos) que puedan asistirlos en este proceso.

El segundo aspecto por considerar es que el impacto final de las tecnologías digitales no ha sido y no será uniforme. Cada empresa reacciona de forma distinta y, en cada caso, puede generarse tanto un impacto positivo que incrementa la competitividad de las empresas, como un impacto negativo que la reduce. La posibilidad de evolucionar en un sentido u otro depende del historial y de la capacidad instalada en las empresas y, especialmente en el caso de las pymes, del rol que desempeñan los distintos actores del ecosistema productivo e institucional en el que las empresas estén insertas y del grado de coherencia de sus actividades de apoyo.

Un esquema interpretativo muy simple, podría considerar dos variables: el grado de especialización de las empresas y el grado de cohesión y dinamismo del sistema productivo en el cual estas operan. En términos generales, debería reconocerse que la digitalización no tiene necesariamente que anular los factores competitivos que permiten a las pymes más calificadas competir de forma exitosa, inclusive en mercados abiertos.

En particular, una de las características que permite a dichas empresas alcanzar niveles importantes de dinamismo, consiste en el dominio de competencias altamente sofisticadas, especialmente en las fases productivas. Estas capacidades se desarrollan mediante aprendizajes en gran medida tácitos (y por lo tanto escasamente permeables a los procesos de digitalización); gracias a procesos de división externa del trabajo, que posibilitan un alto grado de especialización; y en contextos caracterizados por relaciones de confianza muy estrechas entre empresas, instituciones de investigaciones, asociaciones empresariales, entidades de formación técnica, etc. lo que permite la complementación productiva.

Estos sistemas de relaciones conforman capitales intangibles, externos a las empresas individuales, pero internos al territorio de pertenencia, que son fundamentales para el desempeño competitivo de las empresas que los conforman.

La evolución de estos complejos conjuntos de empresas e instituciones es el resultado de un equilibrio inestable que se balancea entre cohesión y apertura: la apertura hacia nuevos sujetos y nuevas ideas, y la cohesión de los actores locales que se identifican con el sistema productivo local al que pertenecen.

La digitalización puede mejorar la cohesión, así como ampliar las posibilidades de apertura de estos sistemas o generar un efecto centrífugo que termina desarticulando el sistema local. Entre los factores que mayormente determinan su evolución y el equilibrio final, está la capacidad de orientación de los líderes locales que, en el caso de sistemas de pequeñas empresas pueden ser: las grandes empresas (en el caso de una integración en cadenas productivas dinámicas) o las instituciones de investigación y apoyo que operan en el territorio, en beneficio del sistema productivo y que asesoran a las empresas más pequeña en la interpretación y adopción de estas tecnologías.

En síntesis, para empresas calificadas e integradas en sistemas dinámicos, es probable que las potencialidades del proceso de digitalización superen las dificultades, abriendo oportunidades reales para reforzar sus estrategias de diversificación y consolidar o ampliar su posición en viejos y nuevos mercados. Estas empresas podrán mejorar la eficiencia de los sistemas de comunicación y logística que las interconectan, desarrollar nuevos servicios comunes, potenciar las plataformas de gestión de las estrategias mancomunadas, perfeccionar los sistemas de control y supervisión para reducir rechazos y tiempos muertos, entre otros.

De no existir un adecuado soporte en estas direcciones, difícilmente los artesanos podrán aprovechar adecuadamente las potencialidades de la tecnología digital. Las pymes que están insertas en sistemas productivos, en funciones escasamente especializadas, gracias a la tecnología digital pueden verse expuestas a una competencia más directa de parte de competidores tecnológicamente más desarrollados, pero, al mismo tiempo, pueden también mejorar su posibilidad de acceso e informaciones y conocimientos, y a instrumentos de up-grade tecnológico.

Las pymes que están insertas en sistemas productivos, en funciones escasamente especializadas, gracias a la tecnología digital pueden verse expuestas a una competencia más directa de parte de competidores tecnológicamente más desarrollados, pero, al mismo tiempo, pueden también mejorar su posibilidad de acceso e informaciones y conocimientos, y a instrumentos de upgrade tecnológico.

Si bien las pymes de estas categorías pueden incrementar el número de sus clientes potenciales, mejorar su gestión de costo o potenciar su capacidad de promocionar sus productos y servicios; al

mismo tiempo, pueden experimentar de forma aún más dramática el impacto de nuevos competidores y especialmente de empresas grandes que, gracias a las nuevas tecnologías, alcanzan una productividad significativamente mayor, una capacidad de producción por pequeños lotes y una enorme flexibilidad que les permite penetrar en todos los mercados anteriormente descuidados por su escaso tamaño.

Un segundo elemento importante es la falta de una estrategia que diferencie los instrumentos o programas de apoyo para la incorporación de las tecnologías digitales según las características de las empresas atendidas. Con la excepción de las políticas que han sido diseñadas, en algunos países de la región, para apoyar a las empresas de las áreas marginales, en general, no existen esfuerzos sistemáticos para adaptar las medidas de apoyo a las distintas necesidades y potencialidades de las empresas.

Un último aspecto por destacar concierne al objetivo predominante en las acciones de fomento de las tecnologías digitales. Los resultados preliminares del estudio que está desarrollando la CEPAL sobre este tema indican que los instrumentos que prevalecen son los que apuntan a incrementar las posibilidades de acceso a Internet y a estimular en los actores el desarrollo de capacidades básicas en el manejo de las tecnologías digitales (alfabetización digital).

La problemática del acceso, que sigue siendo un obstáculo de especial relevancia para la población marginal, especialmente en las zonas rurales más alejadas, se ha enfrentado mediante la acción de apoyo de centros comunitarios, centros empresariales u otras oficinas de atención descentralizada, que ofrecen a las comunidades y a las empresas puntos de contacto a internet e instructivos básicos para el manejo de las herramientas más simples, como navegar en la web, uso del correo electrónico y creación de cuentas personales en las redes sociales.

Mucho más escasos son los programas o las políticas que promueven la incorporación de estas tecnologías en los procesos productivos de las empresas. La transformación digital de una empresa se desarrolla en períodos de tiempo largos y requiere tanto de apoyo técnico como de un financiamiento adecuado. En relación con esto último, tan sólo en la Argentina se identificaron programas de financiamiento explícitamente relacionados con la incorporación de tecnologías digitales. Hay varias iniciativas de fomento del comercio digital, mientras que el uso de las tecnologías digitales para la reconfiguración de las cadenas productivas es aún incipiente y ha tenido lugar en muy pocos países. (fuente - M. Dini y G. Stumpo (coords.), “MiPymes en América Latina: un frágil desempeño y nuevos desafíos para las políticas de fomento”, Documentos de Proyectos (LC/TS.2018/75/ Rev.1), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2020.)

Imagen 5. Principales elementos de debilidad

(Fuente - M. Dini y G. Stumpo (coords.), "MiPymes en América Latina: un frágil desempeño y nuevos desafíos para las políticas de fomento", Documentos de Proyectos (LC/TS.2018/75/ Rev.1), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2020.)

La presencia en internet que tienen las pymes, adaptación de las pymes por la pandemia

La presencia de las pymes en internet hoy en día es más común que hace 5 años, esto debido lastimosamente por la pandemia y el confinamiento que produjo el covid-19 y no por deseo de las pymes; como lo menciona Charles Darwin en su obra el origen de las especies no sobrevive aquel que es más fuerte sino el que mejor se adapta, las pymes tuvieron que evolucionar y adaptarse a la nueva normalidad que se vivía.

Todos los negocios necesitan estar presentes en internet. La pandemia lo ha demostrado. Muchos han podido continuar con su actividad e incluso han descubierto nuevas oportunidades para crecer. Sobre todo, las pequeñas y medianas empresas (pymes) han encontrado en el entorno digital un aliado para resistir el impacto de la crisis sanitaria. Ahora la gran pregunta es cómo lograr el objetivo final de las técnicas de mercado en la red: darse a conocer entre los clientes potenciales y fidelizar a los que ya tienen. (fuente: Jorge G García Claves para que las pymes triunfen en internet, El País El periódico global, 03 NOV 2021, URL: https://elpais.com/economia/estar-donde-estes/2021-11-03/claves-para-que-las-pymes-triunfen-en-internet.html)

Según Rodrigo Miranda, director de la escuela de negocios digitales ISDI, el consumidor dedica mucho tiempo al mundo digital. Allí interactúa, comparte sus gustos y desarrolla buena parte de su vida diaria. Por eso, es el canal idóneo para acercarse a él. Pero para lograrlo hace falta establecer una estrategia y conocer cuáles son las herramientas digitales adecuadas, la mayoría fáciles de usar y que suponen una inversión mínima.

Las industrias en general tuvieron que rápidamente adoptar medidas que salvaguarden su sostenibilidad. El comercio ha mostrado evolución, muchas empresas migraron por completo a un formato digital mientras que otras ampliaron sus canales de venta y servicio. Los consumidores han modificado sus hábitos de compra, a pesar de estar acostumbrados a una experiencia más tangible ha optado por nuevos canales virtuales qué garanticen en algo su seguridad. Las billeteras y aplicaciones móviles cada vez se utilizan con mayor frecuencia como un lugar para realizar compras. (fuente: Vásquez Huiracocha Juan Andrés, El marketing digital como estrategia de las MiPymes en tiempos de pandemia, 2021)

Hoy por hoy el tiempo frente a un celular está en su punto más alto para muchas personas, ya sea por actividades educativas, laborales u ocio los celulares se han convertido en un acompañante del día a día. El marketing digital aprovecha esta realidad, promocionando productos y servicios empresariales a través de internet. de esta manera las empresas pueden aumentar su actividad digital, implementando o mejorando las herramientas actuales para asegurar de que sus esfuerzos de marketing tengan más probabilidades de llegar a los potenciales clientes con el fin de transmitir el mensaje al orientarlos hacia donde pasan la mayor parte de su tiempo.

Cuando se tienen escenarios como el actual y la mayoría de las personas permanecen en sus hogares, el marketing de contenido podría ser un medio eficaz para mantener el contacto con los clientes y aumentar la generación de canalizaciones. Si se emplean las estrategias de marketing de contenido adecuadas, la participación y la comunicación con los clientes pueden permanecer constantes independientemente de cómo se desarrolla la pandemia en los próximos meses.

El confinamiento provocado por la pandemia ha generado una adaptación a la digitalización y el uso de plataformas virtuales por parte de los negocios. Los negocios deben ajustarse en algunos aspectos como mejorar la capacidad de respuesta a la demanda, servir a los clientes de una manera más personalizada, aportar servicios postventa, producir y vender productos en menos tiempo, añadir servicios a los productos físicos y aprovechar la información para su análisis y explotarla en tiempo real. La forma tradicional de realizar marketing tiene que adaptarse al internet para realizar comercio electrónico con los consumidores que cada vez son más tecnológicos gracias a la cantidad de

información que existe. (fuente: Vásquez Huiracocha Juan Andrés, El marketing digital como estrategia de las MiPymes en tiempos de pandemia, 2021)

Las crisis muchas veces representan quiebras, pero también trae nuevas oportunidades de negocios, replanteamientos del negocio, es por ello la importancia que las empresas desarrollen nuevas estrategias o modelos de negocios para contrarrestar los tiempos malos. Es por ello, que el marketing digital se ha convertido en una herramienta importante para las empresas, haciéndolas más competitivas en el mercado donde el Internet juega un papel fundamental en la competitividad a nivel mundial.

En las MiPymes la digitalización en los procesos y las herramientas de trabajo ha sido y seguirán siendo clave durante esta crisis originada por el COVID-19. Por lo que, las MiPymes deben de contar con la capacidad de adaptarse a situaciones adversas y reconocer que hay una variedad de amenazas futuras que no se pueden predecir, medir adecuadamente, ni conocer los efectos que pueden presentar. Por lo que, es necesario repensar en las prioridades y optimización da la empresa.

Los sistemas nos enseñan a optimizar las cadenas de suministro de la empresa. El marketing digital ha tenido un crecimiento importante en las últimas décadas, debido a que un gran número de empresas que están invirtiendo en estas estrategias y reconocen el alcance que tienen con los clientes en todo el mundo, convirtiéndose en una herramienta importante en las ventas de los productos y servicios en esta crisis originada por el COVID-19 (Marco Alberto Valenzo-Jiménez, Víctor Béjar-Tinoco, Jaime Apolinar Martínez-Arroyo, Estrategias De Marketing Digital En Las PYMES Como Nuevo Paradigma De Los Negocios Después Del COVID-19).

El marketing digital son una serie de estrategias que permiten a las MiPymes ampliar el comercio nacional e Internacional, esto es posible con tener presencia en las redes sociales y contar con una página web para tener un mayor alcance con los clientes. Por lo que, se necesita fortalecer la conectividad nacional, capacitando a los empresarios con el uso de Tecnologías de la Información y Comunicación, así como, en la normatividad en cuanto al Comercio electrónico. Además, las Pymes, deben distinguirse con una propuesta de valor en los contenidos, procurando que sean únicos y que no sea estáticos, contar con vínculos con toda la información que el cliente necesite para satisfacer sus deseos y gustos en los distintos mercados. (Marco Alberto Valenzo-Jiménez, Víctor Béjar-Tinoco, Jaime Apolinar Martínez-Arroyo, Estrategias De Marketing Digital En Las PYMES Como Nuevo Paradigma De Los Negocios Después Del COVID-19).

Ventajas de las redes sociales: Es un medio que concentra millones de usuarios, administrar el avance sobre el conocimiento de la marca, se puede concientizar la marca y generar confianza, produce nuevos consumidores, extiende el alcance y el dominio, evoluciona vínculos duraderos con los consumidores.

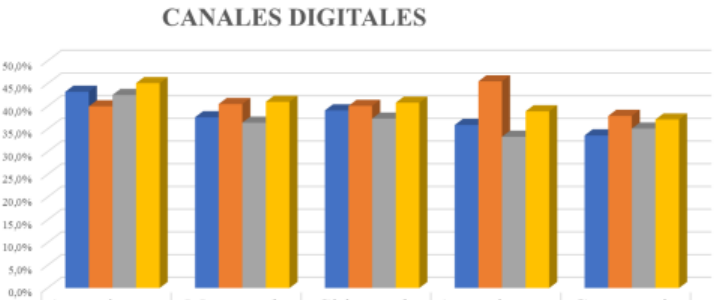
El alcance de las actividades de marketing digital es ilimitado. En comparación con el marketing tradicional, la empresa puede atraer fácilmente la atención de cualquier usuario a un bajo costo.

Entre los usos del marketing digital tenemos los siguientes puntos:

- Aumentar la marca, la presencia y visibilidad.
- Mejorar el posicionamiento en buscadores.
- Mejorar las acciones comerciales.
- Obtener nuevos contactos de clientes y a crear una base de datos.
- Aumentar la presencia en LinkedIn, la plataforma ideal para empresas.
- Comunicar con mensajes claros para llegar mejor a más clientes potenciales.
- Optimizar la página web y otras plataformas.
- Mejorar la vía de comunicación con clientes potenciales.
- Medir los progresos estableciendo indicadores claros en las distintas estrategias de Marketing.
- Reorientar la estrategia para una mejora continua en base a los resultados obtenidos.

(Fuente: Jaime Graneros Segovia, Innovación empresarial de PYMES en tiempo de pandemia, diciembre 2020)

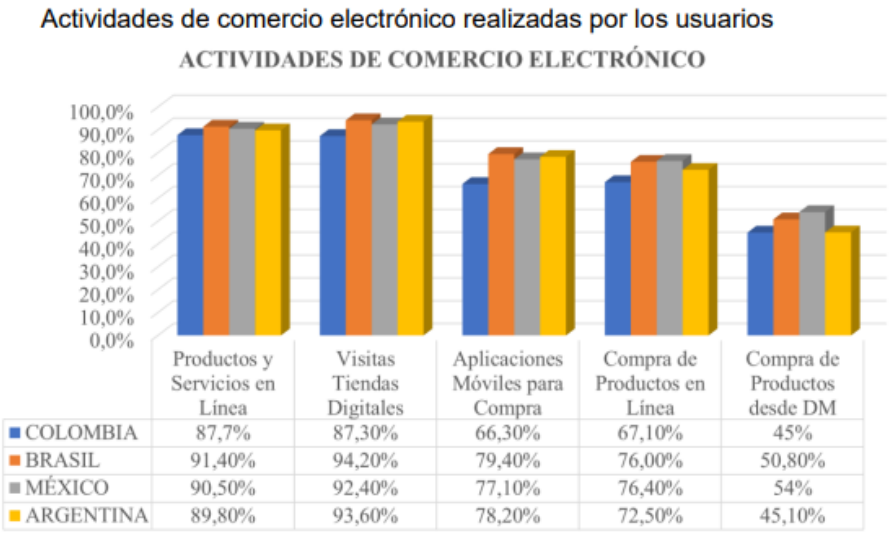
Canales digitales usados por los usuarios para descubrir productos y servicios



	Anuncios en redes sociales	Motores de búsqueda	Sitios web de marca o productos	Anuncios en sitios web	Comentarios en redes sociales
COLOMBIA	43,2%	37,6%	39,1%	35,9%	33,6%
BRASIL	40%	40,5%	40,1%	45,5%	37,9%
MÉXICO	42,5%	36,4%	37,3%	33,3%	35,1%
ARGENTINA	45,1%	41,0%	40,8%	38,9%	37,1%

Imagen 6. Canales digitales usados por los usuarios

(Fuente – adaptado de (Alvino, 2021))



	Productos y Servicios en Línea	Visitas Tiendas Digitales	Aplicaciones Móviles para Compra	Compra de Productos en Línea	Compra de Productos desde DM
COLOMBIA	87,7%	87,30%	66,30%	67,10%	45%
BRASIL	91,40%	94,20%	79,40%	76,00%	50,80%
MÉXICO	90,50%	92,40%	77,10%	76,40%	54%
ARGENTINA	89,80%	93,60%	78,20%	72,50%	45,10%

Imagen 7. Actividades de comercio electrónico

(Fuente – adaptado de (Alvino,2021))

Estadísticas de ataque

Muchos han aprendido por las malas que las pequeñas empresas son objetivos frecuentes de los ciberataques. La idea de "apuntar a una víctima" en sí misma ha quedado en entredicho, y cada vez más personas se dan cuenta de que los ataques generalizados e indiscriminados son a la reputación. En consecuencia, las PYMES son más vulnerables a este tipo de enfoques, ya que suelen carecer de la concienciación, el personal informático interno y la postura cibernética para resistirlos.

La gran mayoría de las empresas siguen siendo vulnerables a los ataques

Según una investigación reciente, betanews nos dice que los ciberdelincuentes pueden penetrar de forma fiable en el 93% de las redes de las organizaciones.

Positive Technologies llevó a cabo una serie de pen tests en varios sectores importantes, como el financiero, el de los combustibles y la energía, los organismos gubernamentales, las empresas industriales e incluso las empresas de TI. Demostraron que, en el 93 por ciento de los casos de prueba, un atacante podía violar las defensas de la red de una organización y obtener acceso a la red local.

Un estudio de CISCO revela que el 40% de las MiPymes que se enfrentaron a un ciberataque experimentaron al menos ocho horas de inactividad. El tiempo de inactividad representa gran parte de los daños financieros globales de una violación de la seguridad.

Además, cada vez hay más ataques dirigidos a las pequeñas y medianas empresas. Mientras que el 43% de los ciberataques van dirigidos a las pequeñas empresas, sólo el 14% se considera preparado,

consciente y capaz de defender sus redes y datos. (Estudio de Accenture sobre el coste de la ciberdelincuencia)

Además, como señala la revista Cybersecurity Magazine:

- el 30% de las pequeñas empresas considera el phishing como su mayor amenaza cibernética
- el 83% de las pequeñas y medianas empresas no están preparadas para recuperarse de los daños financieros de un ciberataque
- el 91% de las pequeñas empresas no ha contratado un seguro de Ciber responsabilidad, a pesar de ser conscientes del riesgo y de la probabilidad de que no puedan recuperarse de un ataque
- Sólo el 14% de las pequeñas empresas considera que su postura de ciberseguridad es muy eficaz

Los humanos siguen siendo explotados como el "eslabón más débil" de un plan de ciberseguridad.

El phishing por correo electrónico, el spear-phishing y la ingeniería social siguen siendo los medios más comunes y fiables para acceder ilegalmente a una red. Más de 12 millones de correos electrónicos de phishing e ingeniería social llegaron a los buzones de más de 17.000 organizaciones estadounidenses sólo en 2021. Además, en el 85% de las infracciones intervino una persona con información privilegiada, y en el 61% de las infracciones se utilizaron contraseñas débiles o credenciales comprometidas.

La ingeniería social y el phishing son los métodos más utilizados. Incluso cuando el software, el hardware y los parches adecuados están en su lugar, el elemento humano sigue siendo un punto débil para la entrada. Como todos sabemos, este vector de ataque sólo se hizo más viable después de la pandemia, ya que muchas empresas recurrieron a modalidades de trabajo remoto y se apresuraron a realizar el proceso de transformación digital como una cuestión de supervivencia. Numerosos estudios han demostrado que el riesgo cibernético aumentó en consonancia con el incremento del trabajo a distancia.

Además, estos informes revelaron:

- el 70% de los trabajadores de oficina utilizan dispositivos de trabajo para tareas personales
- el 37% de los trabajadores de oficina utilizan sus ordenadores personales para acceder a las aplicaciones de trabajo
- el 57% de las violaciones de datos podrían haberse evitado instalando un parche disponible

Estas estadísticas pueden parecer desalentadoras, y muchas pequeñas empresas se sienten impotentes ante estas cifras. Después de todo, las sofisticadas herramientas de ciberseguridad y los expertos

cualificados no son baratos y pueden ser difíciles de justificar, incluso cuando una PYME sabe que un ciberataque podría dejar a su empresa fuera de juego.

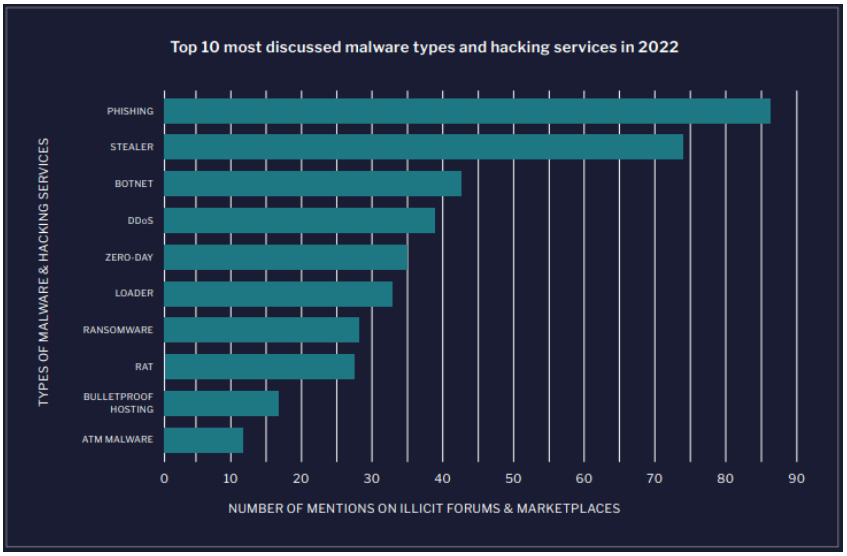


Imagen 8. tipos de malware y servicios de piratería más discutidos

(Fuente: flashpoint, State of Cyber Threat Intelligence, 2023)

Imagen 9. Grupos de ransomware

(Fuente: flashpoint, State of Cyber Threat Intelligence, 2023)

POLÍTICA

En la actualidad la información de las organizaciones se ha reconocido como un activo valioso y a medida que los sistemas de información apoyan cada vez más los procesos de misión crítica se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos.

Esto debido a que los sistemas y la red enfrentan amenazas de seguridad que incluyen, entre muchas otras: el fraude por computadora, espionaje, sabotaje, vandalismo, robo, suplantación y pérdida de información por causa de código malicioso, y tomando en cuenta que cada vez se hacen más comunes, por ello se busca presentar una Política de Seguridad de la Información orientada a cualquier tipo de organización para ayudar a formalizar el compromiso con el proceso de gestión responsable de la información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos misionales., para mayor detalle consultar la política en Anexos.

Gobierno y Auditoria

Gobierno

Debe haber un balance entre la velocidad del negocio y gestionar los riesgos de manera adecuada.

El gobierno corporativo es el conjunto de responsabilidades y practicas ejercidas por el director y la alta gerencia.

En el pasado, considerar la función de TI de una organización como una función meramente de soporte, una función separada y diferenciada del resto del negocio era una práctica común. Actualmente, la mayor parte de la inversión en infraestructura y nuevas aplicaciones de TI abarcan líneas y funciones del negocio. Algunas organizaciones incluso llegan a integrar a socios y clientes en sus procesos internos. Por consiguiente, los CEO's (directores ejecutivos) y los CIO's (directores de TI) cada vez más sienten la necesidad de aumentar las relaciones entre TI y el negocio.

Es necesario un cambio en el rol de TI para extraer el máximo rendimiento a una inversión en TI y usar la tecnología como un arma competitiva.

Si TI se va a gestionar como un negocio dentro del negocio, el concepto de gobierno (proceso en el que se ayuda la gerencia para conseguir sus objetivos) es también aplicable a la gestión de TI.

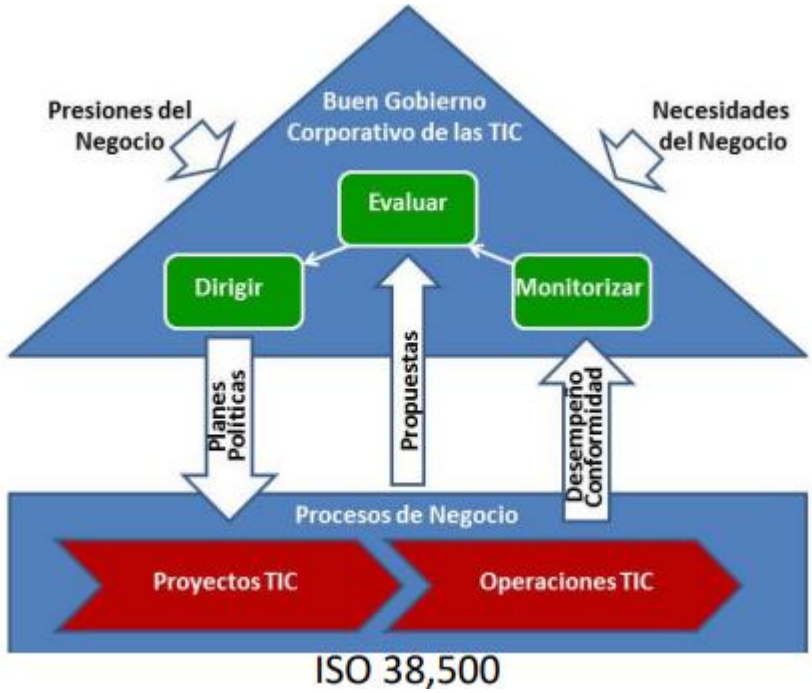


Imagen 10. Gobierno corporativo de las TIC

(Fuente – Auditoria de los sistemas informáticos, Catedra MAESTRIA EN SEGURIDAD Y GESTION DE RIESGOS INFORMATICOS, Universidad Don Bosco 2021)

¿Qué es gobierno de seguridad de la información?

Es un subconjunto del gobierno corporativo, provee dirección estratégica a las actividades de seguridad y asegura que los objetivos sean alcanzados, asegura que el riesgo de seguridad de la información se gestione apropiadamente, también ayuda a asegurar que los recursos de la información son utilizados responsablemente.

El Gobierno Corporativo de TI implica la evaluación y dirección del uso de dicha tecnología para dar soporte a la organización y el monitoreo de este uso para alcanzar los planes. Este incluye la estrategia y las políticas para utilizar la tecnología de la información dentro de una organización.

A fin de lograr un efectivo gobierno de seguridad de la información, la gerencia debe establecer y mantener un marco de trabajo, este marco de trabajo deberá guiar el desarrollo y gestión de un programa de seguridad de la información amplio que soporte los objetivos de negocios.

El marco de trabajo de gobierno generalmente consistirá en:

- Estándares: un conjunto completo para cada política.
- Métricas y procesos: monitoreo para garantizar el cumplimiento y entregar retroalimentación.

- Una estrategia de seguridad: amplia y vinculada con los objetivos del negocio.
- Las políticas de seguridad: que abordan cada aspecto estratégico, controles y regulaciones.
- Una estructura organizacional: libre de conflictos de intereses con la suficiente autoridad y recursos, no puede ser juez ni parte.

Roles y responsabilidades de la alta dirección

- Consejo de dirección/alta dirección: gobierno de seguridad de la información.
- Dirección ejecutiva: implementar un gobierno efectivo de seguridad y definir los objetivos estratégicos de seguridad.
- Comité directivo: asegurar que estén involucradas todas las partes interesadas impactadas por consideraciones de seguridad.
- CISO (Chief Information Security Officer): las responsabilidades van desde el CISO (quien reporta al CEO) hasta los administradores de sistemas que tienen una responsabilidad de part-time por la gestión de la seguridad.

La seguridad de la información requiere:

Desarrollar la estrategia de seguridad con la colaboración de unidades clave del negocio y la aprobación de la estrategia por parte de la alta dirección y educar a la gerencia.

- Comunicación: establecimiento de los canales de reporte y comunicación.
- Liderazgo: liderazgo y respaldo continuo por parte de la alta dirección.
- Sinergias: integración con las gerencias de la unidad de negocio y organizacional, así como de su cooperación.

El GCR (Gobierno Cumplimiento Riesgo): es enfoque adoptado por muchas organizaciones para combinar procesos de aseguramiento que incluyen: auditoría interna, programas de cumplimiento, gestión de incidentes, gestión de riesgos empresariales (ERM).

Un programa de GRC de TI generalmente incluye:

- Librerías de controles y políticas
- Distribución de políticas y respuestas
- Autoevaluación de controles de TI y medición

- Repositorio de activos de TI
- Recopilación automatizada de control de computadoras general
- Gestión de correcciones y excepciones
- Reporte
- Evaluación avanzada de riesgos de TI y tableros de cumplimiento

Gobierno Corporativo

Marco de Referencia para Juntas Efectivas

El marco de referencia de Gobierno Corporativo fue desarrollado para ayudar a las Juntas Directivas a evaluar la efectividad del programa de gobierno de la Organización, considerando:

- Habilidades y Conocimientos
- Procesos
- Información
- Comportamiento

Imagen 11. Marco de referencia para juntas efectivas

(Fuente: Deloitte, Gobierno, Riesgo y Cumplimiento GRC, 2019)

Solución tecnológica para la gestión integrada de riesgos

Estructura integrada de las líneas de defensa

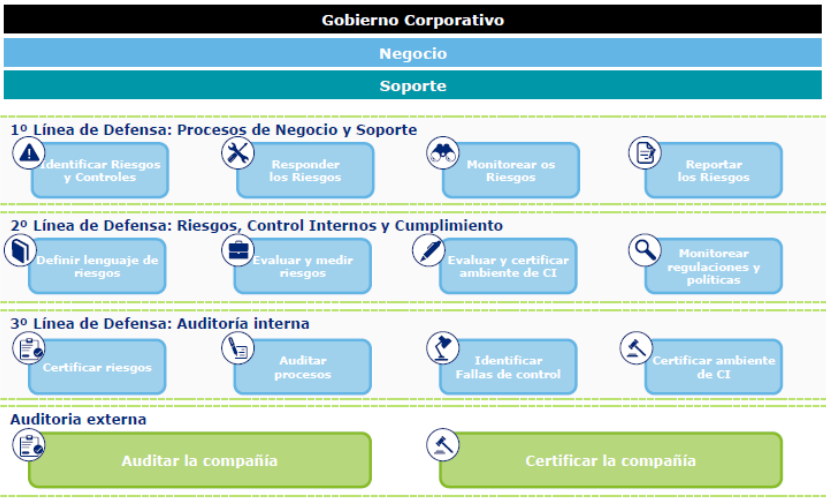


Imagen 12. Estructura integrada de las líneas de defensa

(Fuente: Deloitte, Gobierno, Riesgo y Cumplimiento GRC, 2019)

Marco de la Gestión del Riesgo de Cumplimiento

De extremo a extremo, el marco de la Gestión de Riesgo de Cumplimiento y el modelo operacional relacionado han evolucionado para satisfacer las expectativas aumentadas y establecen una manera estándar de diseñar, evaluar, implementar y mejorar continuamente la función de cumplimiento de una organización para impulsar la modernización.

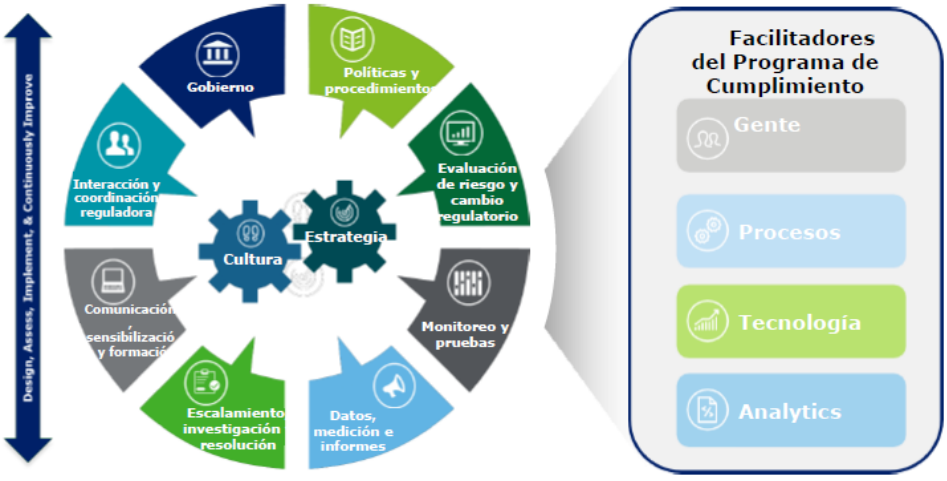


Imagen 13. Marco de la gestión del riesgo de cumplimiento

(Fuente: Deloitte, Gobierno, Riesgo y Cumplimiento GRC, 2019)

Auditoria

Es un proceso formal y necesario para las empresas con el fin de asegurar que todos sus activos sean protegidos en forma adecuada. Asimismo, la alta dirección espera que de los proyectos de auditoría surjan las recomendaciones necesarias para que se lleven a cabo de manera oportuna y satisfactoria las políticas, controles y procedimientos y definidos formalmente, con objeto de que cada individuo o función de la organización opere de modo productivo en sus actividades diarias, respetando las normas generales de honestidad y trabajo aceptadas. (Enrique Hernández, Auditoria de Informática, Un Enfoque Metodológico).

En el ambiente de sistemas, los exámenes de las operaciones que realiza un sistema de cómputo con la finalidad de evaluar la situación del mismo. Los auditores deben tener la capacidad de validar los reportes y de probar la autenticidad y la precisión de los datos y la información que se maneja.

Auditoria se visualiza como un proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de auditoría.

Criterios de auditoria: conjunto de políticas, procedimientos o requisitos utilizados como referencia.

Evidencia de la auditoria: registros, declaraciones de hechos o cualquier otra información que son pertinentes para los criterios de auditoría y que son verificables.

Hallazgos de la auditoría: resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría.

Programa de auditoría: conjunto de una o más auditorías planificadas para un intervalo de tiempo determinado y dirigidas hacia un propósito específico.

Plan de auditoría: descripción de las actividades en sitio y de los preparativos para una auditoría.

Competencia: aptitud demostrada para aplicar conocimientos y habilidades.

Auditoria Informática: La Auditoría Informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

Tipos de auditoria informática

Auditoría de la gestión: la contratación de bienes y servicios, documentación de los programas, etc. **Auditoría legal del Reglamento de Protección de Datos:** Cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos. **Auditoría de los datos:** Clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas.

Auditoría de las bases de datos: Controles de acceso, de actualización, de integridad y calidad de los datos.

Auditoría de la seguridad: referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.

Auditoría de la seguridad física: referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta. También está referida a las protecciones externas (arcos de seguridad, CCTV, vigilantes, etc.) y protecciones del entorno. **Auditoría de la seguridad lógica:** Comprende los métodos de autenticación de los sistemas de información.

Auditoría de las comunicaciones: Se refiere a la auditoría de los procesos de autenticación en los sistemas de comunicación.

Auditoría de la seguridad en producción: Frente a errores, accidentes y fraudes.

Alcance de auditoria

El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoria informática, se complementa con los objetivos de ésta. El alcance ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas.

Control

Los controles se definen como políticas, procedimientos, mecanismos, sistemas y otras medidas diseñadas para reducir el riesgo y asegurar el desempeño deseado.

Objetivos de los controles:

- Proteger los activos de IT
- Precisión de las transacciones
- Confidencialidad y privacidad
- Disponibilidad de los sistemas

- Control de cambios de los sistemas en producción
- Cumplimiento con políticas corporativas

CONFLICTO DE INTERÉS

Los conflictos de interés son aquellas situaciones en las que el juicio del auditor tiende a estar indebidamente influenciado por un interés secundario, de tipo generalmente económico o personal.

Es aconsejable que quien sea responsable de la ética dentro de la firma de auditoría se asegure de que se sigan procedimientos adecuados cuando se identifiquen posibles conflictos de intereses.

Actividades de ejecución de la auditoria

Definir el presupuesto de horas

Con el propósito de ser eficientes, se debe establecer el presupuesto de horas partiendo de la propuesta, es decir, debe ser rentable para el auditor sin dejar de lado la calidad del trabajo y considerando, por tanto, la tarifa/hora por cada una de las categorías que participan en la auditoría.

Reporte de tiempo

Durante el desarrollo de la auditoría, se deben controlar las horas incurridas en cada proyecto por cada uno de los participantes en la auditoría, con el fin de realizar un seguimiento al cumplimiento del presupuesto.

Definir un cronograma de visitas durante el año

Con base en la metodología a desarrollar, se debe definir el cronograma de trabajo (para compartir con el cliente), el cual debe estar alineado con el presupuesto de horas de la propuesta. De acuerdo con la fecha de apertura, las tareas generalmente deben quedar distribuidas en un mes aproximadamente (por ejemplo, 31 de marzo y 30 de abril).

AGENDAS DE REUNIÓN

En la auditoría se debe obtener un entendimiento del negocio; dicho entendimiento, se hace de arriba hacia abajo, es decir que se debe comenzar por entrevistarse con los principales directivos de la compañía, ya que son ellos quienes conocen la operación de la entidad, sus debilidades, oportunidades, fortalezas y amenazas. Por lo anterior, es importante reunirse personalmente con la gerencia y no únicamente por teléfono o por escrito. Se debe programar reuniones con los gerentes de las siguientes

áreas: dirección, administrativa y financiera, ventas, compras, producción, recursos humanos, sistemas y otras que el auditor considere, de acuerdo con la estructura de la compañía y a su enfoque.

El objetivo de estas reuniones es obtener un entendimiento de cómo funciona la organización, con el fin de identificar riesgos de negocio, fraude y procesos y la existencia de respuestas que los mitigan por parte de la gerencia. A mayor entendimiento de la entidad, mayor es la probabilidad de identificar riesgos que puedan afectar el logro de los objetivos de la organización.

Algunos de los temas que se pueden abordar en estas reuniones son:

- Actualizar nuestra compresión del negocio, estructura, personal y cambios de la entidad desde el período anterior.
- Identificar los productos, sus mercados, clientes y alianzas.
- Conocer los objetivos del negocio y su estrategia.
- Identificar cómo miden el logro de sus objetivos.
- Identificar las fuerzas externas que afectan a la organización
- Identificar las fortalezas, oportunidades, debilidades y amenazas.
- Identificar los riesgos del negocio y cómo los administran.
- Entender, evaluar y validar los controles manejados por el gerente-propietario u otro individuo con cargo gerencial.
- Riesgos de fraude.
- Entre otros

Indicadores

Los indicadores de TI son esenciales para medir el rendimiento de los equipos y las actividades realizadas. Las métricas e indicadores de TI optimizan los procesos, mejoran la toma de decisiones, aumentan la productividad y, en consecuencia, los resultados.

Estructurando bien cuáles serán los objetivos de TI y cómo medir este rendimiento, la empresa alcanza todo su potencial. En este contexto, es esencial que los profesionales comprendan esta cultura y sepan desempeñar sus responsabilidades de la mejor manera posible.

¿Qué son los indicadores de TI?

Los indicadores de TI no son más que herramientas de gestión que miden el rendimiento de las actividades realizadas por el equipo de tecnología de la información. Los indicadores se aplican en diversos sectores y evalúan si las acciones emprendidas contribuyen realmente a la consecución de los

objetivos fijados. Cada empresa y cada sector deben encontrar qué indicadores conviene medir para evaluar correctamente los procesos.

Así, los indicadores de TI medirán el impacto del sector en el día a día de la empresa, cuáles son los costos que conlleva y el rendimiento de cada empleado, entre otros.

¿Cómo utilizar los objetivos e indicadores de TI?

Definir correctamente los objetivos e indicadores de TI es muy importante para realizar una correcta medición del negocio. Hay diferentes tipos de indicadores clave.

A continuación, se mencionan algunos como ejemplo:

Tiempo medio entre fallas y tiempo medio de reparación

El tiempo medio entre fallas mide el tiempo invertido en pensar en el funcionamiento de las máquinas. La fórmula para calcular este indicador es:

Tiempo de disponibilidad - tiempo de inactividad / número de fallos. El resultado será igual al tiempo medio entre fallas.

Procesos internos

Normalmente, no hay problemas con la definición de indicadores para procesos de negocio internos. Una buena práctica es rastrear por separado el tiempo de inactividad relacionado con los problemas de seguridad, y crear el plan de prevención respectivo.

Tiempo medio entre fallos (MTBF).

Tiempo medio de la solución (MTTR).

Disponibilidad (tiempo de actividad) calculada como MTBF / (MTBF + MTTR) * 100. Aplicado a los sistemas internos, red, sitio web, etc.

Tasa de éxito de restauración.

Emular el bloqueo del sistema, rastrear el % de datos restaurados y el tiempo de restauración. Esta emulación generará un plan de acción para mejorar el sistema de TI.

Análisis en equipos.

cantidad de servers a los que se le han hecho análisis/cantidad total de servers.

ANEXOS

POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN

Objetivos

- Definir las directrices de la organización para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información.

- Proteger, preservar y administrar objetivamente la información de la organización junto con las tecnologías utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

- Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y auditada dentro del marco determinado por los riesgos globales y específicos de la organización para asegurar su permanencia y nivel de eficacia.

Alcance

Esta política es de aplicación en el conjunto de dependencias que componen la organización, a sus recursos, a la totalidad de los procesos internos o externos vinculados a la organización a través de contratos o acuerdos con terceros y a todo el personal de la organización, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

Generalidades

Según la Norma ISO-27001 ha sido elaborada para suministrar los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. La adopción de un SGSI es una decisión estratégica para cualquier organización. El establecimiento e implementación SGSI de una organización está influenciado por las necesidad y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales, empleados, tamaño, y estructura de la organización.
EL SGSI preserva la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo, y brinda la confianza a las partes interesadas acerca de que los riesgos son gestionados adecuadamente.
Es importante que el sistema de gestión de la seguridad de la información sea parte de los procesos y de la estructura de la gestión total de la información de la organización y que esté integrado con ellos, y que la seguridad de la información se considere en el diseño de los procesos, sistemas de información y controles. Se espera que un SGSI se difunda de acuerdo con las necesidades de cualquier organización.

ISO/IEC 27000, Information Technology. Security Techniques. Information Security Managment Systems.
Tomando como contexto lo anterior es de suma importancia que todas las MiPymes, cuenten con una política de seguridad de la información, a continuación, se presenta un ejemplo de política que podría ser adoptada por cualquier organización:

Términos y Definiciones

- Activo: Cualquier cosa que tiene valor para la organización.

- Análisis de riesgo: Uso sistemático de la información para identificar las fuentes y estimar el nivel del riesgo.

- Autenticidad: Los activos de información los crean, editan y custodian usuarios reconocidos quienes validan su contenido.
- Confiabilidad de la Información: Es fiable el contenido de los activos de información que conserven la confidencialidad, integridad, disponibilidad, autenticidad y legalidad.

- Confidencialidad: Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- Disponibilidad: Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.

- Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

- Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información, o una situación desconocida previamente que pueda ser pertinente a la seguridad.

- Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- Integridad: El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.

- Legalidad: Los activos de información cumplen los parámetros legales, normativos y estatutarios de la organización.

- No repudio: Los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.

- Posibilidad de Auditoría: Se mantienen evidencias de todas las actividades y acciones que afectan a los activos de información.

- Protección a la duplicación: Los activos de información son objeto de clasificación, y se llevan registros de las copias generadas de aquellos catalogados como confidenciales.

- SGSI: Sistema de Gestión de Seguridad de la Información, es un conjunto de principios o procedimientos que se utilizan para identificar riesgos y definir los pasos de mitigación de riesgos que deben llevarse a cabo.

- Spam: se refiere a mensajes no solicitados y no deseados enviados en cantidades masivas.

PROCEDIMIENTOS Y RESPONSABILIDADES

La dirección debe brindar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del sistema de gestión de seguridad de la información; mediante el establecimiento de una política del SGSI, asegurando que se establezcan los objetivos y planes mediante el establecimiento de funciones y responsabilidades de seguridad de la información y comunicando a la organización la importancia de cumplir los objetivos de seguridad de la información; brindando los recursos suficientes para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar el SGSI, decidiendo los criterios para la aceptación de riesgos y los niveles de riesgo aceptables, asegurar a la vez que se realizan auditorias del SGSI y llevando a cabo las revisiones por la dirección.

La gerencia de IT y/o el equipo de las Pymes responsable de ciberseguridad IT y/o el área de seguridad de la información puede en cualquier momento cambiar la prioridad o concluir la ejecución de cualquier proceso del usuario que cree y/o consuma recursos excesivos del sistema o si este uso infringe la política de seguridad.

Documentación de aplicaciones en producción

Previamente a pasar una aplicación al ambiente productivo, el propietario debe haber preparado y autorizado la documentación bajo la metodología de proyectos establecida en la Pymes.

Modificación de Datos y programas

Los datos y programas del ambiente productivo solo pueden ser modificados a través de los procesos y flujos establecidos de la gestión de cambios.

Segregación de funciones clave

Todo proceso debe contar con controles que incluyan la segregación de funciones que garanticen que ninguna persona tendrá el control exclusivo de activos de información.

Procedimiento control de cambios

Se debe emplear un proceso de control de cambios con el fin de autorizar los cambios en el software, hardware, redes y procedimientos relacionados. Este proceso debe de garantizar que todo cambio en la infraestructura productiva cumpla con la documentación, requerimientos, pruebas, calidad, aprobación del propietario y el mismo sea evaluado y autorizado en el comité de cambios establecido.

INTRODUCCIÓN A LA POLÍTICA

En la actualidad la información de la organización se ha reconocido como un activo valioso y a medida que los sistemas de información apoyan cada vez más los procesos de misión crítica se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos.

La organización, los sistemas y red de información enfrentan amenazas de seguridad que incluyen, entre muchas otras: el fraude por computadora, espionaje, sabotaje, vandalismo, fuego, robo e inundación. Las posibilidades de daño y pérdida de información por causa de código malicioso, mal uso o ataques de denegación de servicio se hacen cada vez más comunes. Con la promulgación de la presente Política de Seguridad de la Información la organización formaliza su compromiso con el proceso de gestión responsable de información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos misionales.

Acerca de la Seguridad de la Información

La seguridad de la información se entiende como la preservación, aseguramiento y cumplimiento de las siguientes características de la información:

.

Organización para la Seguridad de la Información

La organización garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información, del cual hace parte integral la presente política, por medio de la creación de una comisión técnica denominada Comité de Seguridad de la Información cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

- Director o un delegado especializado,
- Gerente o un delegado especializado
- Subgerente o un delegado especializado
- Jefe de la Oficina o un delegado especializado
- Jefe de Datos o un delegado especializado

Asesor certificado en seguridad de la información.

En todo caso, dicha comisión o la mesa de trabajo dependerá de la estructura organizacional, las necesidades de la empresa y deberá revisar y actualizar anualmente esta política presentando las propuestas a las directivas de la organización para su aprobación mediante.

Identificación, clasificación y valoración de activos de información.

Cada dependencia, bajo supervisión del Comité de Seguridad de la Información, debe elaborar y mantener un inventario de los activos de información que poseen (procesada y producida). Las características del inventario, donde se incorpore la clasificación, valoración, ubicación y acceso de la información, las especifica el Comité de Seguridad de la Información, correspondiendo a la oficina de Sistemas brindar herramientas que permitan la administración del inventario por cada dependencia, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

La Red de Datos en coordinación con la División de Recursos Físicos y la Sección de Almacén tienen la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la organización.

Seguridad de la información en el Recurso Humano

Todo el personal de la organización, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe debe tener asociado un perfil de uso de los recursos de información, incluyendo el hardware y software asociado.
La Oficina de Sistemas en coordinación con la Red de Datos deben mantener un directorio completo y actualizado de tales perfiles.

El Comité de Seguridad de la Información determina cuales son los atributos que deben definirse para los diferentes perfiles. El Comité de Seguridad de la Información debe elaborar, mantener, actualizar, mejorar y difundir el manual de "Responsabilidades Personales para la Seguridad de la Información en la "organización".

La responsabilidad de custodia de cualquier archivo mantenido, usado o producido por el personal que se retira, o cambia de cargo, recae en el jefe de departamento; en todo caso el proceso de cambio en la cadena de custodia de la información debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

Control de Acceso

Todo el personal de la organización, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y las tareas que desempeñe debe firmar un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de TI y las reglas y perfiles que autorizan el uso de la información institucional.
Los procedimientos para obtener tales perfiles y las características de cada uno de ellos deben ser mantenidos y actualizados por cada dependencia, de acuerdo a los lineamientos dados por la Oficina de sistemas, en cuanto a la información y la Red de Datos, en cuanto a los dispositivos hardware y los elementos software.
La organización debe contemplar procesos y sanciones disciplinarias para los casos en que se presente usos de información y TI que violen los términos y condiciones.
La Oficina de Recursos Humanos junto con la Oficina de Sistemas se encargarán de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información que propenda por el crecimiento continuo de la conciencia individual y colectiva en temas de seguridad de la información.
La Oficina de Sistemas en conjunto con la Red de Datos se encargarán de crear y mantener un centro documental de acceso general con información relacionada con temas de seguridad de la información tales como responsabilidad en la administración de archivos, buenas prácticas, amenazas de seguridad, entre otros.

Responsabilidades de los empleados

Para poder usar los recursos de TI de la organización, los empleados deben leer y aceptar los términos y condiciones. La Oficina de Sistemas debe asegurar los mecanismos para la difusión y aceptación de dichas condiciones por medio de registros y manuales en línea.
El reglamento debe contemplar procesos y sanciones disciplinarias para los casos en que se presente usos de información y TI que violen los términos y condiciones.

Responsabilidades de Usuarios Externos

Todos los usuarios externos y personal de empresas externas deben estar autorizados por una Política de Seguridad de la Información miembro del personal de la Organización quien será responsable del control y vigilancia del uso adecuado de la información y los recursos de TI institucionales. Los procedimientos para el registro de tales usuarios deben ser creados y mantenido por la Oficina de Sistemas en conjunto con la Red de Datos y la Oficina de Recursos Humanos.

Los usuarios externos deben aceptar por escrito los términos y condiciones de uso de la información y recursos de TI institucionales. Las cuentas de usuarios externos deben ser de perfiles específicos y tener caducidad no superior a tres (3) meses, renovables de acuerdo a la naturaleza del usuario.

POLÍTICAS GENERALES PARA USUARIOS DE LOS ACTIVOS DE INFORMACIÓN

Seguridad Física y del entorno

Se debe tener acceso controlado y restringido a los cuartos de servidores principales, subsidiarios y a los cuartos de comunicaciones. La Red de Datos en conjunto con la Oficina Asesora de Sistemas elaborarán y mantendrán las normas, controles y registros de acceso a dichas áreas.

Control de Acceso a los Sistemas

Todo empleado al que se le otorgue un código de usuario (o login), con su respectiva contraseña, o cualquier otra forma de acceso autorizado, es responsable de su uso y protección, estos son únicos e intransferibles.

Acceso remoto a la red

El acceso remoto a la red y a los recursos de la organización será permitido sólo cuando los usuarios autorizados son autenticados, la información viaje encriptada a través de la red y los privilegios sobre la misma sean restringidos.

Seguridad en los equipos

Los servidores que contengan información y servicios institucional deben ser mantenidos en un ambiente seguro y protegido por los menos con:

- Controles de acceso y seguridad física.
- Detección de incendio y sistemas de extinción de conflagraciones.
- Controles de humedad y temperatura.
- Bajo riesgo de inundación.
- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

ADMINISTRACIÓN INCIDENTES Y OPERACIONES

Reporte e investigación de incidentes de seguridad

El personal de la organización debe reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad a través de su jefe de dependencia a la Oficina de Sistemas o la Red de Datos. En casos especiales dichos reportes podrán realizarse directamente a la Oficina de Sistemas, la cual debe garantizar las herramientas informáticas para que formalmente se realicen tales denuncias.

PROTECCIÓN CONTRA SOFTWARE MALICIOSO Y HACKING

Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque multinivel que involucre controles humanos, físicos técnicos y administrativos.

Copias de Seguridad

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo con los procedimientos documentados por el Comité de Seguridad de la Información. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

Administración de Configuraciones de Red

La configuración de enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad y mantenida por la Red de Datos. Todo equipo de TI debe ser revisado, registrado y aprobado por la Red de Datos antes de conectarse a cualquier nodo de la Red de comunicaciones y datos institucional. Dicha dependencia debe desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.

Internet y Correo Electrónico

Las normas de uso de Internet y de los servicios de correo electrónico serán elaboradas, y actualizadas por el Comité de Seguridad de la Información y en todo caso este comité debe velar por el cumplimiento del código de ética institucional y el manejo responsable de los recursos de tecnologías de la información.

INSTALACIÓN DE SOFTWARE

Inventario de Software

Corresponde a la Oficina de Sistemas en conjunto con la Red de Datos mantener una base de datos actualizada que contenga un inventario del software autorizado para su uso e instalación en los sistemas informáticos institucionales.

Computación Móvil

La organización reconoce el alto grado de exposición que presenta la información y los datos almacenados en dispositivos portátiles (computadores portátiles, notebooks, PDA, celulares, entre otros).

Corresponde a la Oficina de Recursos Humanos en conjunto con la Oficina de Sistemas elaborar, mantener e implementar planes de capacitación que propendan por la formación y mantenimiento de la conciencia en cuestión de seguridad de la información.

Las redes inalámbricas potencialmente introducen nuevos riesgos de seguridad que deben ser identificados, valorados y tratados de acuerdo a los lineamientos de la Política de Seguridad en redes inalámbricas que debe elaborar el Comité de Seguridad de la Información.

AUDITORIA Y SEGUIMIENTO

Todo uso que se haga de los recursos de tecnologías de la información en la organización debe ser seguidos y auditados de acuerdo con los lineamientos del Código de Ética y del Código de Uso de Recursos de Tecnologías de la Información, el cual debe ser elaborado por el Comité de Seguridad de la Información.

Administración de Continuidad del Negocio

La Administración de Continuidad del Negocio debe ser parte integral del Plan de Administración de Riesgo de la Organización.

GESTIÓN DE VULNERABILIDADES

Con el fin de mitigar la materialización de riesgos y eventos disruptivos por la existencia de vulnerabilidades en los dispositivos de red, se deben ejecutar pruebas de vulnerabilidad para cualquier equipo que contiene información institucional, servidor nuevo o aplicación de manera previa a su puesta en producción. Las pruebas se llevarán a cabo de acuerdo a lo definido por la gerencia de IT o por la solicitud de las áreas de la organización, el análisis de vulnerabilidades y la categorización de vulnerabilidades fueron realizadas tomando como referencia los controles CIS y la metodología de medición CVE, para brindar un mejor detalle sobre la periodicidad de ejecución de los análisis según el riesgo en cada equipo, la categorización o ponderación del riesgo y el tiempo de remediación según el nivel de criticidad.

Análisis del riesgo

Análisis de vulnerabilidades por equipos

Tabla 3. Análisis de vulnerabilidades por equipos

Tipo de equipo	Periodo	Nivel de Riesgo
Expuesto a internet	3 meses	Alto
Dentro de red interna	6 meses	Medio
Con información sensible	3 meses	Alto
Con información publica	12 meses	Bajo
Dentro de DMZ	3 meses	Alto

Fuente: Elaboración propia para Implementación de estándar CIS para escaneo de vulnerabilidades en granja de servidores Windows

Categorización de vulnerabilidades

Tabla 4. Categorización de vulnerabilidades

Escala	Rango	Descripción	Tiempo de remediación
Bajo	0.1-3.9	Representa las vulnerabilidades que tienen una naturaleza informativa o de preocupación	360 días
Medio	4.0-6.9	Estas vulnerabilidades suponen un riesgo mínimo para la seguridad de los datos	180 días
Alto	7.0-8.9	Estas vulnerabilidades deben revisarse y remediarse siempre que sea posible	90 días
Critico	9.0-10.0	Estas vulnerabilidades deben priorizarse para la remediación inmediata	45 días

Fuente: Elaboración propia sobre la base de NIST, National Vulnerability Database, Vulnerability Metrics, https://nvd.nist.gov/vuln-metrics/cvss

Excepciones

Si por algún motivo justificado IT no puede cumplir con sus obligaciones deberá de justificar por escrito y utilizando un canal oficial de comunicación a las partes involucradas; dentro de las excepciones permitidas tenemos las siguientes:

- Equipo debe pasar a producción sin contar con el análisis previo de vulnerabilidades, esto aplica únicamente para equipos que se coloquen dentro de la red interna, a la vez deberán de hacerlo del conocimiento del Gerente de IT, y deberán de solicitar en un plazo no mayor a 30 días calendario el análisis de vulnerabilidades para dicho equipo.
- Equipo no cuenta con los últimos parches de seguridad disponibles antes de pasar a producción, esto aplica únicamente para equipos que se coloquen dentro de la red interna, a la vez deberán de hacerlo del conocimiento del Gerente de IT, y deberán de aplicar los últimos kb en un plazo no mayor a 60 días calendario.

Cualquier excepción a la presente política de la seguridad de la información deberán ser registradas e informadas al responsable de la seguridad de la información y partes interesadas que correspondan.

Estas excepciones serán analizadas para evaluar el riesgo que podrían introducir a la organización y en base a la categorización de estos riesgos, estos deberán ser asumidos por el solicitante de la excepción junto con los responsables del negocio.

Nota: Cualquier equipo expuesto a internet se excluye de estas excepciones.

CUMPLIMIENTO

Todo uso y seguimiento de uso a los recursos de TI en la Organización debe estar de acuerdo con las normas y estatutos internos, así como a la legislación nacional en la materia, incluido, pero no restringido a:

- Leyes locales
- Normas técnicas internacionales (ISO)
- Entes reguladores
- Entre otros.

PROCEDIMIENTOS

introducción

En el presente documento se detallan los procedimientos a tomar en consideración para su respectiva implementación o adopción como buena práctica por parte de cada Pyme, el desarrollo de cada procedimiento fue hecho en base a la Política de la seguridad de la información ya antes descrita y que forma parte del trabajo de investigación general.

Los procedimientos fueron realizados tomando en cuenta directrices que las pymes tienen aplicadas en su respectiva organización, estos procedimientos están orientados a robustecer y proteger la información que las pymes consideren critica, se ha tratado de cubrir cada arista de la seguridad de la información para garantizar que la infraestructura informática tenga lo mínimo requerido para proteger los activos y reducir el riesgo en caso de que alguno se materialice.

Objetivos

- Definir las directrices de la organización para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información.

- Proteger, preservar y administrar objetivamente la información de la organización junto con las tecnologías utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

- Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y auditada dentro del marco determinado por los riesgos globales y específicos de la organización para asegurar su permanencia y nivel de eficacia.

Alcance

Esta política es de aplicación en el conjunto de dependencias que componen la organización, a sus recursos, a la totalidad de los procesos internos o externos vinculados a la organización a través de contratos o acuerdos con terceros y a todo el personal de la organización, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

Seguridad Física y del entorno

Se debe tener acceso controlado y restringido a los cuartos de servidores, subsidiarios y a los cuartos de comunicaciones. La Red de Datos en conjunto con la Oficina Asesora de Sistemas elaborarán y mantendrán las normas, controles y registros de acceso a dichas áreas.

1. Los visitantes deben autenticarse: se debe registrar su fecha y hora de entrada / salida.
2. Monitorización: Las actividades deben ser monitoreadas de acuerdo con el proceso a realizar.
3. Comunicación: Se debe informar a los trabajadores que acceden sobre los procedimientos de seguridad y emergencia (especialmente en el caso de los centros de datos) y se les debe otorgar acceso para fines específicos.
4. Identificaciones: Al personal que trabaje en áreas seguras se le debe exigir llevar identificación y cualquier persona que no use la identificación requerida debe ser notificada a los empleados de seguridad.
5. Revisión de permisos: Los derechos de acceso deben revisarse periódicamente y revocarse según corresponda.

Externos

1. Personal Externo: Si hay personal externo autorizado y realizan el trabajo sin ser acompañados por personal propio en una sala de servidores o centro de datos, debemos asegurarnos de que el acceso a otras áreas esté bloqueado y que todo el cableado esté seguro. Se aconseja realizar una inspección física de las instalaciones al finalizar los trabajos.
2. Prohibir los trabajos sin supervisión que vayan a ser realizados o ejecutados por parte de terceros.
3. Prohibir el uso de móviles / cámaras a no ser que estén expresamente autorizados.

Entorno

1. Evitar accesos no necesarios
2. Proteger los equipos de áreas sensibles como centros de datos o salas de servidores
3. Medidas de protección contra daños eléctricos (fuentes de alimentación reguladas, líneas de alimentación separadas y respaldadas etc.)
4. Control medioambiental para cumplir con las especificaciones del fabricante en cuanto a condiciones de humedad, temperatura protección contra polvo o materiales que puedan dañar los equipos
5. Deben establecerse pautas para comer, beber y fumar cerca del equipo para evitar daños o simplemente evitar que los empleados estén en contacto con los equipos si no están trabajando en ellos.
6. En cuanto a las instalaciones deben diseñarse para evitar al máximo posible el riesgo que la información confidencial sea accesible para los visitantes y personas no autorizadas.
7. Se debe realizar el debido mantenimiento a los equipos, esto debe ser realizado por personal calificado.
8. Se debe llevar el control de los mantenimientos realizados y en agenda los próximos a realizar.

Control de Acceso a los Sistemas

Todo empleado al que se le otorgue un código de usuario (o login), con su respectiva contraseña, o cualquier otra forma de acceso autorizado, es responsable de su uso y protección, estos son únicos e intransferibles.

1. Crear perfiles de trabajo para el personal que labora en la institución, esto debe ser en conjunto con el área de reclutamiento, recurso humano o similar.
2. Todas las aplicaciones o sistemas utilizados en la institución deben tener clave de acceso.
3. Se deben crear perfiles de usuarios para el ingreso a las aplicaciones o sistemas de la institución.
4. Prohibir imprimir, anotar y compartir usuarios y claves de acceso.
5. El administrador del control de accesos deberá cambiar inmediatamente las claves de acceso a los empleados o contratistas que tengan ausencias definitivas de sus cargos o terminación de sus contratos.
6. Cuando una persona sea removida de su cargo ya sea por renuncia o despido, el jefe inmediato de la persona debe hacer entrega del equipo a su cargo y de los usuarios de sistemas.
7. Queda prohibida la utilización de cualquier recurso informático y de la Red para almacenar o portar material ilegal, pornográfico, que haga apología del crimen o violencia, ofensivo al buen nombre y honor de otros, propagandas comerciales, cadenas, difusión de actividades lucrativas en general, o su utilización en actividades no relacionada con las funciones propias del cargo.
8. Queda prohibida la instalación de hardware y/o software sin la autorización apropiada del área de ciberseguridad.
9. No permitir a personal externo acceder información de la Red sin la autorización de la Unidad de Desarrollo Tecnológico.
10. Las pruebas de penetración son actividades exclusivas del área de ciberseguridad y queda prohibida esta actividad para toda persona que intente descifrar contraseñas. interceptar protocolos de comunicación, utilizar técnicas de escucha, transmisión, grabación o reproducción de cualquier señal de comunicaciones, utilizar la red para intentar ganar el acceso no autorizado a la información local o remota, congestión de enlaces o sistemas informáticos.
11. Queda prohibida la utilización de cualquier software o hardware que pueda comprometer la seguridad de la red y/o de cualquier recurso informático de la misma.
12. Queda prohibida la introducción intencionada de virus, caballos de Troya, gusanos o cualquier otro software perjudicial o nocivo.
13. Queda prohibido el acceso a Internet con fines comerciales o recreativos.
14. Efectuar revisiones periódicas con el objeto de:
    - inhabilitar cuentas inactivas por más de 60 días
    - eliminar cuentas inactivas por más de 120 días

Claves

1. Los usuarios tienen la obligación de cambiar periódicamente su clave de acceso, de acuerdo a los lineamientos establecidos por el área de ciberseguridad, se recomienda establecer un periodo de 4 o 6 semanas.
2. Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto.
3. Almacenar las contraseñas sólo en sistemas informáticos protegidos y autorizados
4. Criterios para las claves:

a. Las contraseñas deben tener una longitud no menos de 8 caracteres.

b. Debe contener al menos:

1 letra mayúscula.

1 letra minúscula.

1 carácter especial.

c. Suspender o bloquear permanentemente al usuario luego de 3 intentos de entrar con una contraseña incorrecta.

d. impedir que las últimas 12 contraseñas sean reutilizadas.

Acceso remoto a la red

El acceso remoto a la red y a los recursos de la organización será permitido sólo cuando los usuarios autorizados son autenticados, la información viaje encriptada a través de la red y los privilegios sobre la misma sean restringidos.

1. Se debe firmar NDA (Acuerdo de Confidencialidad) y requerimientos entre las partes para contratos que requieran acceso remoto.
2. Se debe identificar el usuario que dispondrá de esta modalidad y los permisos de acceso remoto de que dispondrá, por ejemplo (consulta, administración, pruebas, desarrollo, etc.).
3. Toda conexión remota debe ser solicitada, autorizada y registra para posterior control de vigencia. Se evalúa el modelo de conexión, con el objetivo de discriminar el nivel de seguridad necesario a implementar en la conexión.
4. Utiliza el software definido como el estándar de conexión remota, salvo que el área de ciberseguridad indique otro tipo de conexión.
5. Los accesos remotos están sujetos a las fechas de inicio y finalización de cada proyecto comprometido por la Institución.
6. Se debe utilizar método de conexión segura, con método de identificación, cifrado fuerte y autenticación robusta.
7. Las conexiones remotas, deben ser monitoreadas en forma permanente mediante procesos definidos y revisadas periódicamente, en su vigencia.
8. Configura los servidores de acceso remoto para aplicar políticas

Seguridad en los equipos

Los servidores que contengan información y servicios institucional deben ser mantenidos en un ambiente seguro y protegido por los menos con:

- Controles de acceso y seguridad física.
- Detección de incendio y sistemas de extinción de conflagraciones.
- Controles de humedad y temperatura.
- Bajo riesgo de inundación.
- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

1. Toda información en formato digital debe ser mantenida en servidores aprobados por la Oficina de Sistemas o la Red de Datos.

2. El Comité de Informática y Telecomunicaciones define el límite de responsabilidades de las dependencias.

3. No se permite el alojamiento de información institucional en servidores externos sin que medie una aprobación por escrito del Comité de Seguridad de la Información.

4. Equipos claves de comunicaciones deben ser alimentados por sistemas de potencia eléctrica regulados y estar protegidos por UPS.

5. La Red de Datos debe asegurar que la infraestructura de servicios de TI está cubierta por mantenimiento y soporte adecuados de hardware y software.

6. Las estaciones de trabajo deben estar correctamente aseguradas y operadas por personal de la organización el cual debe estar capacitado acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional.

7. Los medios que alojan copias de seguridad deben ser conservados de forma correcta de acuerdo con las políticas y estándares que para tal efecto elabore y mantenga el Comité de Seguridad en la Información.

ADMINISTRACIÓN INCIDENTES Y OPERACIONES

Reporte e investigación de incidentes de seguridad

El personal de la organización debe reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad a través de su jefe de dependencia a la Oficina de Sistemas o la Red de Datos. En casos especiales dichos reportes podrán realizarse directamente a la Oficina de Sistemas, la cual debe garantizar las herramientas informáticas para que formalmente se realicen tales denuncias.

1. El Comité de Seguridad de la Información debe preparar, mantener y difundir las normas, procesos y guías para el reporte e investigación de incidentes de seguridad. En conformidad con la ley, la organización podrá interceptar o realizar seguimiento a las comunicaciones por diferentes mecanismos previa autorización del Comité de Informática y Telecomunicaciones, y en todo caso notificando previamente a los afectados por esta decisión.

2. La Oficina Asesora de Sistemas en conjunto con la Red de Datos mantendrá procedimientos escritos para la operación de sistemas cuya no disponibilidad suponga un impacto alto en el desarrollo normal de actividades. A dichos sistemas se debe realizar seguimiento continuo del desempeño para asegurar la confiabilidad del servicio que prestan.

PROTECCIÓN CONTRA SOFTWARE MALICIOSO Y HACKING

Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque multinivel
Que involucre controles humanos, físicos técnicos y administrativos.

1. El Comité de Seguridad de la Información elaborará y mantendrá un conjunto de políticas, normas, estándares, procedimientos y guías que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking.

2. En todo caso y como control mínimo, las estaciones de trabajo de la Organización deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus. Los usuarios de las estaciones no están autorizados a deshabilitar este control.

3. La organización a través de la Oficina de Sistemas o la Red de Datos podrá hacer seguimiento al tráfico de la red cuando se tenga evidencias de actividad inusual o detrimentos en el desempeño. La dependencia que realice dicho seguimiento deberá informar a la organización a través de correo electrónico o noticias en el portal institucional de la ejecución de esta tarea.

4. La Red de Datos y la Oficina de Sistemas deben mantener actualizada una base de datos con alertas de seguridad reportadas por organismos competentes y actuar en conformidad cuando una alerta pueda tener un impacto considerable en el desempeño de los sistemas informáticos.

Copias de Seguridad

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados por el Comité de Seguridad de la Información. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

1. Las dependencias de la organización deben realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.
2. Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin.
3. La Oficina de Sistemas debe proveer las herramientas para que las dependencias puedan administra la información y registros de copias de seguridad.
4. La Oficina de Control Interno debe efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.
5. Las copias de seguridad de información críticas deben ser mantenida de acuerdo a cronogramas definidos y publicados por la Oficina de Sistemas en conjunto con la Red de Datos.
6. La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios.
7. Los usuarios deben entregar al respectivo jefe de dependencia las copias de seguridad para su registro y custodia.

Administración de Configuraciones de Red

La configuración de enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad y mantenida por la Red de Datos.

Todo equipo de TI debe ser revisado, registrado y aprobado por la Red de Datos antes de conectarse a cualquier nodo de la Red de comunicaciones y datos institucional. Dicha dependencia debe desconectar

aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.

1. Se debe administrar y controlar las redes para proteger la información en sistemas y aplicaciones.
2. Se debe identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados.
3. Se debe segregar las redes en función de los grupos de servicios, usuarios y sistemas de información.
4. Documentar la topología de red, la documentación sobre topología ayuda a entender y utilizar mejor la red.
5. La documentación sobre la topología debería incluir la documentación lógica y física, incluida la conectividad, el direccionamiento, tipos de medios, dispositivos, esquemas de bastidores, asignaciones de tarjetas, ruteo de cables, identificación de cables, puntos de terminación, información de alimentación e información de identificación de circuito.
6. Verificaciones de la integridad de la configuración de la red, La verificación de la integridad de la configuración debe evaluar la configuración general de la red, la complejidad y coherencia, y los problemas potenciales.
7. Establecer periodos de actualización de software y hardware.

Internet y Correo Electrónico

Las normas de uso de Internet y de los servicios de correo electrónico serán elaboradas, y actualizadas por el Comité de Seguridad de la Información y en todo caso este comité debe velar por el cumplimiento del código de ética institucional y el manejo responsable de los recursos de tecnologías de la información.

Correo

1. El uso de correo está autorizado exclusivamente para fines relacionados al cargo que ocupa cada trabajador dentro de la empresa.
2. Se deben establecer medidas de vigilancia y control del contenido enviado, si el envío es externo las medidas y controles deben ser más estrictos y considerar la posibilidad de rechazarlo.
3. El área de ciberseguridad debe informar a los trabajadores acerca de las medidas de control y vigilancia adoptadas en cada caso, motivando la necesidad de la lectura de los correos electrónicos en la protección del patrimonio de la empresa y del resto de los trabajadores.

4. Queda prohibido el envío de correo del tipo spam, suplantación de identidad, cadenas sociales, publicidad u otro correo con relación a esto.
5. El envío de archivos por correo o compartidos por medio drive de forma externa debe ser autorizado previamente y el contenido del archivo será evaluado para determinar si no es información sensible que pueda comprometer a la empresa.
6. Las peticiones de información por parte de entes externos de control deben ser aprobadas por la Dirección ejecutiva y Financiera, y dirigida por dichos entes a los responsables de su custodia.

Internet

1. Se deben crear perfiles de navegación dependiendo del cargo que ocupa cada trabajar.
2. Se debe restringir al trabajador la navegación por Internet para evitar tener que controlar y vigilar su uso por parte del trabajador.
3. Se debe bloquear el acceso a direcciones de internet que estén dedicadas a la pornografía, venta de armas, venta de drogas, tráfico de órganos y de humanos, juegos, apuestas, ocio, descargas no autorizadas y cualquier otro que aplique que no sea para el desarrollo de las actividades laborales.
4. Las restricciones de navegación deben ser del conocimiento de los trabajadores, así como los motivos de dicha limitación de acceso.

INSTALACIÓN DE SOFTWARE

Inventario de Software

Corresponde a la Oficina de Sistemas en conjunto con la Red de Datos mantener una base de datos actualizada que contenga un inventario del software autorizado para su uso e instalación en los sistemas informáticos institucionales.

1. El designado como administrador de software (persona o área) debe estar actualizado con la información sobre el software y el hardware utilizados en toda la organización.
2. Se debe administrar licencias de software, categoría y cumplimiento.
3. Se debe detectar, bloquear y desinstalar el software identificado como prohibido en la red.
4. Se debe tener identificado la fecha de instalación y desinstalación del software.
5. Todas las instalaciones de software que se realicen sobre sistemas de la organización deben ser aprobadas por la Oficina de Sistemas o la Red de Datos, de acuerdo con los procedimientos elaborados para tal fin por dichas dependencias.
6. El Comité de Informática y Telecomunicaciones definirá el ámbito en el cual actuará cada dependencia. No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor.
7. La Oficina de Sistemas y la Red de Datos deben desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad que debe ser investigado.
8. Para apoyar los procesos operativos y estratégicos la organización debe hacer uso intensivo de las Tecnologías de la Información y las Comunicaciones. Los sistemas de software utilizados pueden ser adquiridos a través de terceras partes o desarrollados por personal propio.

9. La Oficina de Sistemas debe elegir, elaborar, mantener y difundir el “Método de Desarrollo de Sistemas Software en la organización” que incluya lineamientos, procesos, buenas prácticas, plantillas y demás artefactos que sirvan para regular los desarrollos de software internos en un ambiente de mitigación del riesgo y aseguramiento de la calidad.
10. Todo proyecto de desarrollo de software interno debe contar con un documento de Identificación y Valoración de Riesgos del proyecto. La Organización no debe emprender procesos de desarrollo o mantenimiento de sistemas software que tengan asociados riesgos altos no mitigados.
11. Los sistemas software adquiridos a través de terceras partes deben certificar el cumplimiento de estándares de calidad en el proceso de desarrollo.

Computación Móvil

La organización reconoce el alto grado de exposición que presenta la información y los datos almacenados en dispositivos portátiles (computadores portátiles, notebooks, PDA, celulares, eentre otros).

Corresponde a la Oficina de Recursos Humanos en conjunto con la Oficina de Sistemas elaborar, mantener e implementar planes de capacitación que propendan por la formación y mantenimiento de la conciencia en cuestión de seguridad de la información.

Las redes inalámbricas potencialmente introducen nuevos riesgos de seguridad que deben ser identificados, valorados y tratados de acuerdo con los lineamientos de la Política de Seguridad en redes inalámbricas que debe elaborar el Comité de Seguridad de la Información.

1. Las computadoras portátiles asignadas a los trabajadores deben tener cifrados la cuenta de usuario o el disco duro completo para evitar que la información que reside en dichas computadoras pueda ser utilizada en caso de pérdida o robo del equipo.
2. Las computadoras portátiles asignadas a los trabajadores deben tener una cuenta de tipo usuario para el uso de los colaboradores y restringido el uso de la cuenta de Administrador y sus privilegios.
3. Todos los equipos computacionales móviles administrados y bajo posesión de la institución deben tener instalado el sistema operativo con todos los parches de seguridad y los parches de las diferentes aplicaciones instaladas que estén disponibles hasta la fecha.
4. Los equipos computacionales móviles deben recibir mantenimiento solo por el área técnica.
5. Queda prohibido que cualquier trabajador que no sea del área técnica abra o intente abrir equipos computacionales móviles para dar algún tipo de mantenimiento o extracción de componentes.

AUDITORIA Y SEGUIMIENTO

Todo uso que se haga de los recursos de tecnologías de la información en la organización debe ser seguidos y auditados de acuerdo con los lineamientos del Código de Ética y del Código de Uso de Recursos de Tecnologías de la Información, el cual debe ser elaborado por el Comité de Seguridad de la Información.

1. Se debe planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.

Administración de Continuidad del Negocio

La Administración de Continuidad del Negocio debe ser parte integral del Plan de Administración de Riesgo de la Organización.

1. La institución debe determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre.
2. La institución debe establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas.
3. La institución debe verificar regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas.
4. Se debe implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.

GESTIÓN DE VULNERABILIDADES

Con el fin de mitigar la materialización de riesgos y eventos disruptivos por la existencia de vulnerabilidades en los dispositivos de red, se deben ejecutar pruebas de vulnerabilidad para cualquier Host, servidor nuevo o aplicación de manera previa a su puesta en producción. Las pruebas se llevarán a cabo de acuerdo con lo definido por la gerencia de IT o por la solicitud de las áreas de la organización.

1. Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
2. Los eventos de seguridad de la información se deben informar lo antes posible utilizando los canales de administración adecuados.
3. Se debe anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización.
4. Se deben evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.
5. Se debe responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.
6. Se debe utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro.
7. La institución debe definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.

Conclusiones

- En el presente trabajo se pudo constatar que el estándar CIS en su versión ocho es el más indicado para la implementación de controles orientados a seguridad en cualquier MiPymes, tomando en cuenta que estas se encuentran en una etapa inicial en cuanto a la gestión de ciberseguridad, CIS ofrece una clasificación de los controles según el tamaño y la madures de las empresas para la implementación, lo que facilita que las empresas no se sientan abrumadas durante la etapa de implementación de los controles, ya que la implementación se hace de manera gradual.

- Se ha comprobado que en ocasiones las organizaciones no cuentan con el apoyo de la alta gerencia para los temas de seguridad y ciberseguridad, ya que las MiPymes generalmente se enfocan únicamente en el negocio, dejando de lado la seguridad informática.

Recomendaciones

- Se recomienda a cualquier organización que desee implementar los controles CIS utilizar la versión más actualizada del estándar, con el fin que esta sea una guía durante la etapa de implementación de los controles.

- Todas empresas deben evaluar, y modificar de ser necesario su organización, a la vez contemplar las áreas de seguridad y ciberseguridad informática, mediante la asignación de roles y funciones, esto con el fin de garantizar la correcta planificación, implementación y ejecución de los controles de seguridad informática.

Bibliografía

https://www.cisecurity.org/controls/cis-controls-list
https://nvd.nist.gov/vuln-metrics/cvss
https://learn.cisecurity.org/cis-ram
https://latam.kaspersky.com/blog/pymes-latam-enfrentan-creciente-numero-ciberataques/24950/
https://www.rapid7.com/products/insightvm/
https://gaptain.com/cultura-de-ciberseguridad-empresas-2/
https://blog.wearedrew.co/ciberseguridad/cultura-de-ciberseguridad-por-que-es-importante-crearla-y-fomentarla
https://blog.wearedrew.co/ciberseguridad/que-puede-hacer-una-pyme-en-relacion-a-la-ciberseguridad
https://revistaindustria.com/2021/05/los-mejores-consejos-de-ciberseguridad-para-pymes/
https://publications.iadb.org/es/los-desafios-del-comercio-electronico-para-las-pyme-principales-claves-en-el-proceso-de
https://revistas.ulima.edu.pe/index.php/Interfases/article/view/4876
https://www.kas.de/en/web/regionalprogramm-adela/single-title/-/content/los-efectos-de-la-digitalizacion-inteligencia-artificial-big-data-e-industria-4-0-en-el-trabajo-de-l
https://dialnet.unirioja.es/servlet/tesiscodigo=172547
https://dspace.ups.edu.ec/bitstream/123456789/20675/1/UPS-CT009220.pdf
https://www.riico.net/index.php/riico/article/view/1902/1755
https://repositorio.upeu.edu.pe/bitstream/handle/20.500.12840/3975/Jaime_Trabajo_Bachiller_2020.pdf?sequence=1&isAllowed=y
https://repository.usta.edu.co/bitstream/handle/11634/43017/2022brigithecampos.pdf?sequence=1&isAllowed=y
https://www.ninjaone.com/es/blog/smb-cybersecurity-statistics-2022/
https://flashpoint.io/wp-content/uploads/State-of-Cyber-Threat-Intelligence-Report-2023.pdf
https://dialnet.unirioja.es/servlet/tesis?codigo=291525
https://normaiso27001.es/a11-seguridad-fisica-y-del-entorno/
https://www.transparencia.gob.sv/institutions/mtps/documents/310460/download
https://www.mtt.gob.cl/wp-content/uploads/2018/12/INS-SSI-09.2_v1.0_-_Instructivo_de_Seguridad_para_Acceso_a_Trave%CC%81s_de_Redes_y_Acceso_Remoto.pdf
https://ayudaleyprotecciondatos.es/2020/06/15/acceso-remoto/
https://www.iso27000.es/iso27002_13.html
https://www.cisco.com/c/es_mx/support/docs/availability/high-availability/15111-configmgmt.html
https://www.marzoasesores.es/control-del-uso-del-email-e-internet-a-los-empleados/
https://www.asep.gob.pa/wp-content/uploads/transparencia/articulo_9/9_8-reglas_procedimientos/informatica/P-ASEP-OIT-05_computacion_movil.pdf
https://www.iso27000.es/iso27002_17.html
https://www.iso27000.es/iso27002_16.html
https://otrs.com/es/casos-de-uso/sgsi/
https://www.sydle.com/es/blog/indicadores-de-ti-605a2bd0b7cdda685648b68a
https://bscdesigner.com/es/principales-kpis-de-ti.htm
https://www.udbvirtual.edu.sv/auladigital/pluginfile.php/620246/mod_resource/content/1/Gu%C3%ADa%20Fase%20Pre-Planificaci%C3%B3n%20%281%29.pdf
https://www.udbvirtual.edu.sv/auladigital/pluginfile.php/620244/mod_resource/content/1/Gu%C3%ADa%20Fase%20Planificaci%C3%B3n.pdf