Rol del auditor en la evaluación del cumplimiento de las políticas de seguridad de la información

Lyda Fabiola Castro Pinzón[1]

Resumen

La evaluación de políticas de seguridad, es un proceso riguroso y metódico, donde el auditor tiene como misión verificar los mecanismos que se han implementado en las organizaciones para el cumplimiento de las mismas.

Las políticas se definen como las normas que deben cumplir los actores que participan en las organizaciones y que hacen uso de la información. El incumplimiento de las políticas puede ocasionar perdidas en los activos de datos y afectaciones reputacionales, que en ocasiones puede llegar a comprometer los objetivos organizacionales.

El rol del auditor en la evaluación del cumplimiento de las políticas de seguridad debe estar enfocado en encontrar las debilidades de seguridad y evaluar la gestión del riesgo que realiza la organización, apoyado de técnicas y herramientas de auditoria que le permitan obtener las evidencias necesarias para emitir un

[1] Lyda Fabiola Castro Pinzón, ingeniero de sistemas, egresada de la Fundación Universitaria de San Gil UNISANGIL, estudiante de la Especialización en Auditoria de Sistemas de la Universidad Antonio Nariño. Email: lidafacastro@gmail.com

concepto sobre el cumplimiento de las políticas, la actualización de las mismas y la gestión que se realiza a los riesgos de la organización.

Palabras Claves (Políticas, seguridad informática, riesgos, evaluación, auditoría)

Abstract

The evaluation of security policies is a rigorous and methodical process, where the auditor's mission is to verify the mechanisms that have been implemented in organizations to comply with them.

Policies are defined as the standards that must be met by the actors who participate in organizations and who make use of the information. Non-compliance with policies can cause loss of data assets and reputational damage, which can sometimes compromise organizational objectives.

The role of the auditor in evaluating compliance with security policies should be focused on finding security weaknesses and evaluating the risk management carried out by the organization, supported by auditing techniques and tools that allow him to obtain the necessary evidence to issue a concept on compliance with policies, updating them and the management carried out to the risks of the organization.

Key words (Policies, IT security, risks, evaluation, audit)

Introducción

El articulo desarrollado, hace una introducción sobre el concepto de auditoria de sistemas, cual es el objetivo y lo que se espera del auditor en el proceso, seguido se presenta el perfil que debe tener el auditor de sistemas, las responsabilidades y sobre todas las habilidades que debe poseer para realizar procesos de auditoria.

Se habla sobre la seguridad de los activos de información y las características de confidencialidad, integridad y disponibilidad que se deben garantizar a través del cumplimiento de las políticas de seguridad informática.

De igual forma, se presenta el concepto de políticas de seguridad, el propósito, los elementos claves, la importancia de las mismas, su definición a nivel organizacional y se sugieren algunos criterios que pueden servir de guía para la formulación de las mismas de acuerdo a las particularidades de cada organización.

Por último, se hace énfasis en los aspectos que el auditor debe considerar en la evaluación de las políticas de seguridad de una organización, teniendo como base lo establecido en la norma ISO 27002. Se sugiere por parte del autor una serie de aspectos para realizar una correcta evaluación.

Metodología

El método de investigación es cualitativo y el tipo a utilizar es explicativo descriptivo, a través del cual se pretende conocer, comprender y orientar los

aspectos que se deben tener en cuenta por parte del auditor de sistemas, para evaluar el cumplimiento de las políticas de seguridad de la información en una empresa.

Se tomará como referente las normas ISO 27001 (ISO/IEC, 2007) y la norma ISO 31000, a través de la cual se establecerá la guía del auditor para evaluar el cumplimiento de las políticas de seguridad, la efectividad de las mismas y la gestión de riesgos en la empresa.

Resultados y discusiones

La auditoría de sistemas, es un proceso realizado por profesionales el cual busca revisar la aplicación de normas, políticas, técnicas y procedimientos, en el área de tecnología de las empresas y evaluar la efectividad de los controles preventivos, los cuales se formalizan a través de políticas que se formulan al interior de la organización, controles detectivos y correctivos establecidos en los diferentes procesos de auditoria, con el fin de conocer si los procesos tecnológicos se realizan de manera eficiente y segura, de tal forma que le permitan a la empresa contar con las disponibilidad, integridad y efectividad de los datos para la toma de decisiones.

Los procesos de auditoria de sistemas, son apoyados con herramientas definidas en la técnica a utilizar por parte del auditor. El uso de diferentes herramientas, permiten aprovechar lo mejor de ellas, y adecuarlas a las necesidades específicas de evaluación, que requiere el ambiente objeto de auditoria.

Para alcanzar resultados óptimos durante la realización de un proceso de auditoría, es importante que el auditor tenga una formación sólida sobre tecnologías y comunicaciones, de tal forma que pueda establecer un criterio claro en la

planeación y desarrollo de la auditoria. Los resultados de la auditoria, se enriquecen con la experiencia del auditor.

El auditor de sistemas

El auditor de sistemas, es un profesional especializado y certificado, con conocimiento en las diferentes ramas de las tecnologías de la información y las comunicaciones, en asuntos legales y la gestión empresarial, capaz de analizar y evaluar los sistemas de información y la infraestructura tecnológica de una organización, con el objetivo de mejorar y sostener los procesos tecnológicos y el cumplimiento de las normas. (White, 2019)

La realización de una auditoría de sistemas, se fundamenta en normas establecidas enfocadas a direccionar los aspectos a contemplar en la misma, las cuales son emitidas por la Organización Internacional de Normalización ISO (ISO/IEC, 2007), el Consejo Normativo de la Asociación de Auditoría y Control de Sistemas de Información, Information Systems Audit and Control Association, (ISACA, 2020), la organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI) (Fiscalizadoras, 2020) y otros estándares establecidos como ITIL, COSO, COBIT, NIAS, que apoyan la labor del auditor de sistemas.

El papel de un auditor de sistemas implica desarrollar, implementar, probar y evaluar los procedimientos de revisión bajo el estándar de auditoria establecido por la organización.

El auditor, busca encontrar las debilidades tecnológicas, las amenazas que pueden llegar a impedir el cumplimiento de los objetivos del negocio y evalúa la gestión de riesgos, de los objetivos de auditoria.

Los auditores son responsables de comunicar sus hallazgos a otros en la organización, esta actividad se realiza a través de la construcción del informe de auditoría.

La calidad de los informes finales, los cuales deben estar siempre basados en la objetividad e imparcialidad, además, dependen de la experiencia obtenida por el auditor en su vida profesional, las habilidades cognitivas y sus capacidades para obtener los mejores resultados de la auditoria, analizando con fluidez y agilidad las situaciones de debilidad o fortaleza de los diferentes entornos del área de tecnología, logrando de esta forma construir un informe de calidad, donde la alta dirección pueda conocer los hallazgos de la auditoria, y las recomendaciones dadas para mejorar o cambiar los procesos y/o sistemas (acciones de mejora e implementación de controles) en pro de garantizar la seguridad y el cumplimiento de los objetivos corporativos. (Sánchez & Florez Gomez, 2018)

Habilidades del auditor

Las habilidades y destrezas que posea el auditor le permitirán desempeñar su trabajo con naturalidad y profesionalismo, enfrentando con facilidad las situaciones que se le presenten durante el desarrollo de la auditoría, permitiéndole obtener toda la información necesaria para la emisión de un juicio objetivo, siempre sustentado en hechos demostrables a través de evidencias. (Raffino, Concepto.de, 2020)

Las habilidades de un auditor, variarán según su función y campo de acción. Sin embargo, el auditor debe contar entre otras, con las siguientes habilidades mostradas en la tabla 1:

Tabla 1. Habilidades del auditor

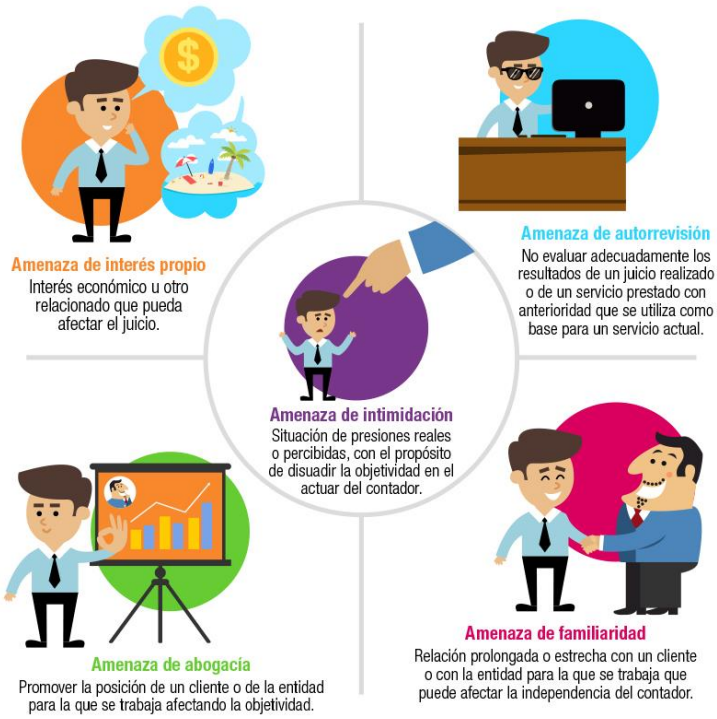
Habilidad	**Descripción**
Autoconocimiento	Capacidad para conocerse a sí mismo y saber cómo es y cómo reacciona.
Empatía	Capacidad para percibir, entender e incluso compartir los sentimientos ajenos.
Comunicación asertiva	habilidad de transmitir información a los demás, de manera rápida, eficaz y precisa.
Toma de decisiones	La capacidad de decidir, rápida o pausadamente, pero eligiendo el criterio más conveniente dadas las opciones presentes.
Pensamiento creativo	Capacidad de hallar soluciones innovadoras a los problemas.
Pensamiento crítico	es la capacidad de analizar, interpretar y desarrollar sus propias conclusiones.
Manejo de problemas y conflictos	Es la capacidad de negociación, flexibilidad y entendimiento en pro de beneficio mutuo.
Manejo de emociones	es la capacidad de darse cuenta, aceptar fácilmente y controlar con éxito los sentimientos en uno mismo
Habilidades cognitivas	Aquellas que involucran los procesos mentales, como la memoria, la rapidez del pensamiento, la deducción lógica o el manejo de lenguajes formales.
Habilidades sociales	Aquellas que involucran el trato con los demás o la comunicación con otros individuos.

Fuente: elaboración propia de acuerdo a las definiciones tomadas de: (Raffino, Concepto.de, 2020)

En el ejercicio de su actividad, el auditor debe tener independencia absoluta para expresar sus opiniones y conceptos sin el riesgo de que pueda ser manipulado de algún modo, se comprometa su credibilidad y confianza y se afecte la calidad del juicio del proceso de auditoría. En otras palabras, el auditor debe ser independiente tanto de hecho como de apariencia. (Gerencie.com, 2017)

Las normas de independencia del auditor establecen un marco de principios, apoyados por una combinación de prohibiciones, restricciones, otras políticas, procedimientos y revelaciones, que aborden al menos las siguientes amenazas a la independencia, representadas en la figura 1: autorrevisión, familiaridad, abogacía, Interés propio, intimidación. (Ltd, 2019)

Figura 1. *Amenazas a la independencia del auditor*



Fuente: https://actualicese.com/amenazas-que-pueden-comprometer-al-contador-en-un-proceso-de-auditoria/

La independencia del auditor es importante para que la opinión expresada en el informe de auditoría pueda ser imparcial, libre de cualquier influencia indebida o conflicto de intereses que anule el juicio profesional del mismo.

(corporatefinanceinstitute, 2015)

Seguridad de la información

La información constituye uno de los activos principales de una organización, por lo tanto, se debe proteger, mediante la construcción de políticas, procedimientos y controles, que se implementan en base a recursos humanos, de hardware y software.

La gestión de la seguridad de la información debe ser un proceso continuo, que parte del establecimiento del contexto, la evaluación y tratamiento de los riesgos, y la construcción de planes de mejora en los cuales se implementen las recomendaciones y decisiones dadas en los diferentes procesos de evaluación. En este ciclo de gestión del riesgo es fundamental que la organización refleje los resultados de la evaluación en la actualización de las políticas de seguridad, teniendo presente que las políticas representan las reglas de actuación por parte de los diferentes usuarios, de esta forma el ciclo de mejora se enriquece y la organización logra cumplir sus objetivos en cuanto a seguridad informática.

(Velasco, 2019)

El rol del Auditor de TI en la evaluación de las Políticas de Seguridad de la Información

En relación con las políticas de seguridad de la información el auditor de TI, debe validar que los controles establecidos en las políticas de seguridad permitan proteger los siguientes criterios de la información presentados en la figura 2:

Figura 2. *Criterios de la información*

Fuente: elaboración propia

El logro de este objetivo, depende de planear la evaluación del cumplimiento de las políticas de seguridad de la información, ejecutar los procedimientos de evaluación, elaborar el informe de resultados de la evaluación y comunicar los resultados a la organización, considerando los siguientes aspectos y escenarios sobre las Políticas de Seguridad, que deben ser objeto de análisis.

Políticas de seguridad

Para abordar la amenaza "interna" a la información y los sistemas de informáticos, con frecuencia se recomienda establecer políticas de seguridad de la información como medida organizativa.

Las políticas de seguridad, son un conjunto de directrices de actuación, que pretenden, a través del cumplimiento de las mismas, velar por la seguridad de la información, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la misma y minimizar los riesgos que pueden afectar una organización.

Las políticas de seguridad se definen en el nivel estratégico, teniendo una alta comprensión de las necesidades especiales de la organización, deben incluir los aspectos que se deben proteger y que son de alto impacto, y estar alineadas a las estrategias de la organización, así como a los estándares internacionales, se desarrollan con el apoyo de manuales y procedimientos de actuación.

La definición de una política se fundamenta en la identificación y análisis de los riesgos que pueden afectar la información, contemplando todos los procesos, recursos de hardware, software, ambientes y equipos de trabajo. (Peltier, 2004)

Por lo tanto, las políticas de seguridad deben estar enfocadas a responder las siguientes inquietudes: *¿Cuáles son los activos que se deben proteger? ¿Cuáles son las amenazas que rodean los activos*? y *¿de qué forma se pueden proteger los activos?*.

Las políticas de seguridad deben ser aprobadas al interior de la organización, por lo general, esta labor es realizada por la gerencia o la junta directiva de la misma, una vez aprobadas deben ser comunicadas y socializadas a todo el personal.

El área de tecnología y la auditoria interna son las encargadas de velar por que las políticas se cumplan y se actualicen de forma periódica, de acuerdo a lo establecido en el ciclo de mejora continua. (Camelo, 2010)

Es importante tener claro, que las políticas de seguridad no son destinadas únicamente al personal de tecnología, si no que están dirigidas a todos los usuarios, de los servicios tecnológicos tanto internos como externos, que sean susceptibles de producir algún error o descuido de seguridad.

Las políticas se formulan, de acuerdo a la particularidad y a las necesidades de las organizaciones, sin embargo, se sugiere tener presente los siguientes criterios para la creación de las mismas. (Duigan, 2003)

Figura 3. *Criterios para la creación de políticas de seguridad*

1. **Identifique los activos a proteger:** realice una lista y clasifique los activos más importantes de la organización
2. **Identifique los riesgos:** ¿Cuáles son los riesgos y las amenazas a los que están expuestos los activos principales de la organización?
3. **Clasifique y estime los riesgos:** ¿Cuánto afecta una falla de seguridad en la organización?, ¿Cuál es la probabilidad de ocurrencia?, priorice los riesgos de mayor impacto. Construya la matriz de riesgos.
4. **Especifique controles:** ¿Determine cuáles son las reglas que se deben cumplir para proteger los activos identificados?
5. **Escriba las políticas:** Documente las reglas y controles establecidos a través de políticas de cumplimiento, tenga presente que las políticas cumplan con los requisitos legales que se requieran.
6. **Apruebe las políticas:** Formalice las políticas mediante la aprobación por parte de la alta dirección de la organización.
7. **Socialice las políticas:** una vez aprobadas comunique y socialice las políticas con los empleados de la organización. Se sugiere realizar procesos de capacitación con el fin de asegurar que todo el personal ha entendido las políticas establecidas. Deje evidencia escrita del proceso.
8. **Establezca sanciones por incumplimiento**: Disponga de un conjunto claro de procedimientos que especifiquen las sanciones por infracciones en las políticas de seguridad y aplíquelos cuando sea necesario
9. **Actualice las políticas:** Establezca una periodicidad para revisar los controles establecidos a los riesgos identificados y las nuevas amenazas que surjan y actualice las políticas de acuerdo al resultado de esta evaluación.
10. **Actualice al personal:** Construya una estrategia para que mantenga actualizado al personal de la empresa con los cambios que se den en las políticas.
11. **Adquiera e implemente los recursos necesarios:** para garantizar el cumplimiento de las políticas se hace necesario adquirir e implementar diferentes herramientas tanto de hardware como de software, que le permitan cumplir con el propósito de protección de la información.

Fuente: elaboración propia

En virtud de lo anterior, para evaluar el cumplimiento de las políticas de seguridad, el auditor debe, debe conocer los recursos con los que cuenta la organización, las amenazas que pueden poner en riesgo la información, y el origen de las mismas que puede ser interno o externo.

Además, el auditor debe constatar que las políticas establecidas sean tomadas por los empleados como "*las reglas que se deben respetar y cumplir para acceder a la información y a los recursos tecnológicos*"; también, debe evaluar el cumplimiento, la efectividad de las políticas en el aseguramiento de la información, y el nivel de actualización que se le haya dado a las mimas, debe considerar que el documento sea dinámico y que haya tenido cambios y mejoras de acuerdo a las situaciones que se presenten en la organización. (Baskerville, 2002)

Políticas asociadas a la seguridad de la información que el auditor debe evaluar.

La seguridad de la información, recoge una gran cantidad de políticas, cuyo objetivo principal es el de establecer un esquema de seguridad claro y transparente bajo la responsabilidad del equipo de Tecnología, en la administración del riesgo, y lograr el compromiso de todo el personal de la organización con el proceso de seguridad, cumpliendo con la aplicación de los controles. (Mesquida, 2012)

Tomando como referente los dominios de seguridad de la norma ISO 27002, se enuncian las principales políticas de seguridad de la información, a tener en

cuenta por el auditor y los aspectos a considerar para evaluar cumplimiento y control de las mismas. (ISO/IEC, 2007)

Políticas de seguridad

1. Política de gestión de las políticas de seguridad.
2. Política de organización de la seguridad de la Información
3. Política de Seguridad de los Recursos Humanos
4. Política de Gestión de Activos
5. Política de Control de Acceso
6. Política de seguridad Física y Ambiental
7. Política de Cifrado
8. Política de Seguridad lógica
9. Política de respaldo de la información
10. Política de adquisición, desarrollo y mantenimiento de sistemas
11. Política de gestión con proveedores
12. Política de Gestión de incidentes de seguridad de la información

En la evaluación de políticas de seguridad, el auditor debe verificar los controles existentes para cada una de las políticas, y el aporte de las mismas en la matriz de riesgos del proceso.

En la tabla 2, se presenta una sugerencia de aspectos a tener en cuenta por parte del auditor, en el momento de evaluar el cumplimiento de las políticas de seguridad de la organización.

Las consideraciones presentadas son una base, sobre lo que se puede evaluar, no significa que sea lo único.

Tabla 2. Aspectos para evaluar el cumplimiento de las políticas de seguridad de la información

Política	**Aspectos a auditar**
Política de gestión de las políticas de seguridad.	• Existencia de políticas • Resolución de aprobación de las políticas. • Evidencias de la comunicación y socialización de las políticas • Evidencias de los procesos de revisión y actualización de las políticas, (versionamiento) • Evidencias de auditorías realizadas a los dominios cubiertos por las políticas.
Política de organización de la seguridad de la Información	• Roles y responsabilidades de los encargados de los procesos de seguridad en la organización. • Matriz de riesgos asociados a la seguridad de la información, el auditor debe hacer especial énfasis en la gestión que se da a los riesgos, y a los planes de mejora establecidos. • Se debe verificar que las políticas de seguridad deben estar alineadas con la estrategia de la organización y los objetivos misionales.
Política de Seguridad de los Recursos Humanos	• El auditor debe validad que el equipo de trabajo encargado de los procesos de seguridad de la información cuente con la experiencia y formación requerida para el cargo (Hoja de vida, títulos, certificados, experiencia en el cargo). • El auditor debe validar los planes de capacitación proyectados y realizados al recurso humano de la empresa, enfocados a promover la importancia de la seguridad. • El auditor debe validar el tratamiento que se le da a los casos de incumplimiento de las políticas de seguridad en la organización, por parte de los funcionarios. • El auditor debe verificar que en los contratos de trabajo se establezca una cláusula donde se especifique que el funcionario reconoce y se acoge a las políticas de seguridad y manejo de la información establecidas por la organización.
Política de Gestión de Activos	• La existencia de un inventario de los activos y que estos estén clasificados y asignados a un responsable (tener en cuenta procesos de desvinculación de personal).

	• La evidencia del monitoreo periódico a los usuarios y sus perfiles de acceso (Trazas, informes, revisión de logs etc.) • El cumplimiento de controles de seguridad como antivirus, sistema operativo actualizado y licenciado, para ello puede hacer uso de alguna de las herramientas de auditoria o un muestreo aleatorio al parque informático. • El cumplimiento de controles de legalidad de uso de software, para ello revisará el inventario de licencias de la organización frente al software instalado en los equipos de cómputo y servidores. • Que la organización cuente con un inventario de software permitido en los equipos de cómputo asignados a los usuarios y los controles que ha establecido para verificar el cumplimiento. • La existencia de un manual, procedimiento o tablas de retención de documentos, donde se clasifique la información y se establezcan los periodos de retención y la disposición de los mismos. • La organización cuente con una directiva de bloqueo de equipo cada cierto tiempo. • La existencia de medios de almacenamiento y resguardo de la información. • Los procedimientos y evidencias de ejecución, de los procesos de eliminación y borrado seguro de información. • Los protocolos de seguridad establecidos a nivel de redes, bases de datos sistemas de información que busquen, asegurar la confidencialidad, disponibilidad e integridad. • La utilización de protocolos y herramientas para la creación de claves, cifrado y resguardo de las mismas.
Política de Control de Acceso	**Físico** • Validar la implantación de mecanismos de seguridad física, controles de acceso físicos. • Contar con áreas seguras en la organización, que sean reconocidas y que tenga las medidas de seguridad requeridas. **Lógico** • La existencia de procedimientos y controles establecidos para proteger el acceso a la red de datos de la organización. • La existencia de un procedimiento para la gestión de cuentas de usuarios (creación, modificación, bloqueo o borrado), donde se especifiquen los niveles de autorización, el proceder en cada caso y los acuerdos de confidencialidad respectivos. • Los formatos de entrega de cuentas de acceso, firmados por los usuarios finales, donde se especifiquen las autorizaciones y acuerdos respectivos. • La existencia de mecanismos de autenticación para las redes inalámbricas de la empresa.

	• La existencia de herramientas seguras para realizar conexiones remotas a la empresa a través de VPN. • Validar que se estén efectuando de forma periódica, procesos de verificación de usuarios y roles. • Evidenciar la existencia de un documento en el cual se plasmen las responsabilidades de acceso de los usuarios a los sistemas, las acciones realizadas en los mismos, así como la responsabilidad en el manejo de contraseñas que le hayan sido asignadas. • Validar que este documento se haya socializado y firmado por el personal, por lo general se recomienda que repose en la hoja de vida del funcionario. • Validar mediante alguna herramienta de auditoria, los controles establecidos para proteger los servicios de información de intentos de inicio de sesión fallidos. • Validar la efectividad de los controles establecidos a nivel de red. • Validar las directivas establecidas para el bloqueo de sesión por inactividad en los equipos de cómputo (usuarios desatendidos). • Validar los controles y la efectividad de los mismos, para asegurar que el acceso al código fuente de los aplicativos.
Política de seguridad Física y Ambiental	• La existencia de Controles de ingreso de hardware que no pertenece a la organización. • La existencia y el cumplimiento de procedimientos para el ingreso a los centros de cableado y centros de datos (áreas seguras, validar bitácora que se lleve.). • El cumplimiento de las condiciones físicas y medioambientales requeridas para la protección y correcta operación de la infraestructura tecnológica. (sistemas de refrigeración, de extinción de incendios, vigilancia, monitoreo, control de acceso, protección eléctrica entre otros.) • La existencia de un cronograma de mantenimiento y el cumplimiento del mismo. • Validar que solo el personal de TI este autorizado para mover equipos el control físico de los activos. • Validar la existencia y cumplimiento de un procedimiento de disposición final de los equipos que han cumplido su vida útil. • Validar las condiciones de seguridad del cableado estructurado de la organización.
Política de Cifrado	• La existencia de mecanismos o herramientas para asegurar la protección de claves de acceso a la red de datos, los sistemas de información, datos y servicios de la organización. • La existencia de herramientas de cifrado, que permitan asegurar la trasmisión de información. • El uso de los mecanismos y herramientas de cifrado de información.

Política de Seguridad lógica	• Validar la topología de la red y la segmentación de la misma. • La utilización de protocolos y herramientas para la creación de claves, cifrado y resguardo de las mismas. • Validar mediante alguna herramienta de auditoria, los controles establecidos para proteger los servicios de información de ataques informáticos. • Validar los controles y la efectividad de los mismos, para asegurar que el acceso al código fuente de los aplicativos. • Validar la aplicación de la política de escritorio limpio. • Validar los controles establecidos para controlar la instalación de software por parte de los usuarios en los equipos de cómputo. • Validar los controles existentes para la protección de la información del equipo de trabajo asignado al usuario final. • Validar la existencia de manuales y procedimientos relacionados con la operación y administración de los sistemas de información. • Validar la separación de ambientes para los sistemas de información (desarrollo, pruebas y producción) • Validar que se realice monitoreo a los recursos informáticos asignados, de tal forma que se realicen las gestiones necesarias para asegurar las capacidades y el rendimiento de los sistemas de información. • Validar que se tenga instalado en los equipos un antivirus • Validar las políticas de control de acceso a los servidores • Validar las políticas de gestión de puertos en servidores. • Validar que la red de datos este segmentada • Validar que se tengan definidos acuerdos de niveles de servicios • Validar que la organización cuente con la protección de equipos de seguridad perimetral. • Validar que se realice control de contenidos • Validar que se realice monitoreo y control del uso del servicio de internet.
Política de respaldo de la información	• La existencia y cumplimiento de una política de respaldo para las bases de datos, aplicaciones en servidores, equipos activos de red, entre otros. • Verificar que se hayan establecido los mecanismos y los procedimientos a seguir para realizar estos respaldos. • Verificar la realización de los backups • Verificar que se tengan establecidos periodos de retención para el respaldo y almacenamiento de la información. • Verifica los procesos de custodia que se realiza a las copias de seguridad • Verificar la existencia de procedimientos de restore de las copias de seguridad, con el fin de validar la eficacia del proceso de backup.
Política de Adquisición, desarrollo y	• Existencia y aplicación del procedimiento para la adquisición de bienes y servicios.

mantenimiento de sistemas	• Existencia y aplicación de una metodología clara para el desarrollo de software que incluya aspectos como requerimientos, estándar de desarrollo, arquitectura, aspectos de seguridad, entre otros aspectos. • Cumplimiento de las fases de ciclo seguro de desarrollo de software. • Procedimientos realizados por la empresa para realizar las migraciones de software. • Verificar los acuerdos, contratos de licenciamiento y condiciones de uso de software desarrollado por terceros. • Verificar los procesos de actualización, y aplicación de parches a los sistemas de información.
Política de gestión de proveedores	• Verificar la existencia de contratos vigentes en los que se especifiquen los alcances del servicio y la responsabilidad de las partes. • Verificar la existencia de acuerdos de Confidencialidad de información, en el cual se incluyan las responsabilidades tanto civil como penal derivada del proceso.
Política de Gestión de incidentes de seguridad de la información	• Verificar que se identifiquen y reporten los incidentes de seguridad. • Verificar que se tengan establecidos responsabilidades y procedimientos de respuesta frente a los incidentes de seguridad que se presenten. • Verificar que se haga seguimiento a los controles establecidos para mitigar los incidentes de seguridad que se hayan presentado.

Fuente: elaboración propia de acuerdo a las definiciones tomadas de: (ISO, 2005)

Finalmente, el rol del auditor durante la auditoria al cumplimiento de las políticas de seguridad, es el de verificar que:

- Los riesgos tecnológicos han sido identificados en la organización
- Que se han diseñado políticas, que regulan las acciones a cumplir por parte del personal para evitar la materialización de los riesgos
- Que existen, y se cumplen los procedimientos que se deben seguir en caso de ocurrencia de un evento disruptivo
- Y que se hace gestión control y gestión de los riesgos.

El auditor debe comprobar a través del análisis de riesgos, que las políticas de seguridad contemplan todos los dominios identificados para garantizar, la confidencialidad, integridad y disponibilidad de la información en la organización

Conclusiones

El establecimiento de políticas de seguridad de la información de alta calidad, es una herramienta práctica y útil para gestionar la seguridad de la información de manera eficaz en las organizaciones.

El auditor de sistemas al evaluar de forma correcta e imparcial el cumplimiento de las políticas de seguridad, le brinda a la organización el estado del arte de sus activos tecnológicos enfocados al grado de cumplimiento de la seguridad de la información.

En la evaluación de las políticas de seguridad, el auditor debe considerar que la organización haya establecido un programa de auditoria periódica a las políticas de seguridad, lo cual se considera como una acción preventiva a las situaciones cambiantes que ponen en riesgo la continuidad del negocio.

El auditor debe tener presente en el proceso de auditoría, que el equipo humano de las organizaciones conozcan las políticas y sepan cómo deben proceder como usuarios de los recursos tecnológicos.

Por último, se concluye que es muy importante que el auditor evalué la metodología empleada por la organización para la formulación de las políticas de seguridad, de tal forma que el proceso realizado responda a las necesidades de las mismas.

Referencias

Baskerville, R. S. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management*.

Camelo, L. (2010, 02 20). *seguridadinformacioncolombia.* Retrieved from http://seguridadinformacioncolombia.blogspot.com/2010/02/certificaciones-en-seguridad-cissp-cisa.html

corporatefinanceinstitute. (2015, 02 16). *corporatefinanceinstitute*. Retrieved from https://corporatefinanceinstitute.com/resources/knowledge/accounting/threats-to-auditor-independence/

Duigan, A. (2003, 08 03). *computerworld*. Retrieved from https://www.computerworld.com/article/2572970/10-steps-to-a-successful-security-policy.html

Fiscalizadoras, I. O. (2020). *INTOSAI*. Retrieved from https://www.intosai.org/es/

Gerencie.com. (2017, 10 24). *Gerencie.com*. Retrieved from https://www.gerencie.com/la-independencia-del-auditor.html

ISACA. (2020). Advancing IT, Audit, Governance, Risk, Privacy & Cybersecurity | ISACA. *ISACA*. Retrieved from https://www.isaca.org/

ISO. (2005). *ISO/IEC 27002:2005, Information Technology - Secuirty Techniques - Code of Practice for Information Management Systems - Requirements.* ISO/IEC.

ISO/IEC. (2007). *NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27002* . ICONTEC.

Ltd, A. A. (2019, 12 16). *ukdiss*. Retrieved from https://ukdiss.com/examples/audit-independence-important.php?vref=1

Mesquida, C. L. (2012). *Implantación sistemas de gestión de la seguridad de la información.*

Peltier, T. (2004). *Information security policies and procedures - a practitioner's reference* (2nd ed ed.). Auerbach Publications.

Raffino, M. E. (2020, 07 09). *Concepto.de*. Retrieved from https://concepto.de/habilidad-2/

Sánchez, S. T., & Florez Gomez, A. S. (2018). *AUDITORÍA PARA EVALUAR EL PROCESO DE GESTIÓN DE LA CALIDAD DE DATOS EN LA.* Bogotá: Universidad Católica.

Velasco, W. V. (2019). POLITICAS Y SEGURIDAD DE LA INFORMACION. *Fides et Ratio - Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia*.

Walter, V. V. (2008). POLITICAS Y SEGURIDAD DE LA INFORMACION. *Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia*, 69.

White, S. K. (2019, 3 5). *cio.com*. Retrieved from https://www.cio.com/article/3346029/it-auditor-role-defined.html