Guía de Auditoria

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Guía No. 15

MINTIC vive digital Colombia TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0	06/05/2016	Versión inicial del documento

TABLA DE CONTENIDO

1. DERECHOS DE AUTOR

2. AUDIENCIA

Entidades públicas de orden nacional y territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno en Línea.

3. INTRODUCCIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

En este sentido, dentro del marco de la estrategia de gobierno en línea, se ha elaborado el modelo de seguridad y privacidad de la información, el cual a lo largo de los últimos años se ha ido actualizando en función de las modificaciones de la norma técnica que le sirve de sustento: ISO 27001, así como las mejores prácticas y cambios normativos de impacto sobre el modelo.

A su turno el Modelo de Seguridad y Privacidad de la Información se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

4. JUSTIFICACIÓN

El Ministerio de las Tecnologías de la Información y las Comunicaciones, en concordancia con las actividades de la estrategia de gobierno en línea y con la implementación del modelo de seguridad y privacidad de la información, pone a disposición de las entidades, la siguiente guía, para que puedan tener una línea base durante los análisis en el recorrido de la implementación del modelo de seguridad y privacidad, de esta manera ayudar a proteger los bienes, activos, servicios, derechos y libertades dependientes del Estado.

5. GLOSARIO

- **ACTIVO:** Cualquier cosa que tenga valor para la organización. [NTC 5411-1:2006]
- **CONTROL**: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
- **SEGURIDAD DE LA INFORMACIÓN**. Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.
- **POLÍTICA**. Toda intención y directriz expresada formalmente por la Dirección.
- **RIESGO**. Combinación de la probabilidad de un evento y sus consecuencias. [ISO/IEC Guía 73:2002]
- **ANÁLISIS DE RIESGOS**. Uso sistemático de la información para identificar las fuentes y estimar el riesgo. [ISO/IEC Guía 73:2002]
- **EVALUACIÓN DE RIESGOS**. Todo proceso de análisis y valoración del riesgo. [ISO/IEC Guía 73:2002]
- **VALORACIÓN DEL RIESGO**. Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo. [ISO/IEC Guía 73:2002]
- **GESTIÓN DEL RIESGO**. Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. [ISO/IEC Guía 73:2002]
- **TRATAMIENTO DEL RIESGO**. Proceso de selección e implementación de medidas a para modificar el riesgo. [ISO/IEC Guía 73:2002]

6. OBJETIVOS

La presente guía tiene como finalidad, indicar los procedimientos de Auditoria en el proceso de verificación de la implementación del modelo de seguridad y privacidad de la información.

A partir del entorno y el contexto determinado por la entidad, la auditoria es una fuente de mejora, permitiendo conocer las debilidades para generar fortalezas, a través de la comprobación, seguimiento y evaluación de la mejora continua.

Por lo tanto, se convierte en una herramienta sistemática, independiente, objetiva, documentada, práctica y medible sobre el cumplimiento de los objetivos de la entidad y es allí donde la mejora continua tiene un papel fundamental.

Las auditorias apoyan la toma de decisiones frente al nivel de implementación y complementa el ciclo de mejora continua en relación con el ciclo PHVA.

Se procura que las entidades tengan un enfoque de seguridad en el cual se incluya el desarrollo y mantenimiento de la misma, realizando mejoras en las áreas que se requiera.

Dependiendo de la entidad, dichos procedimientos pueden variar o si la entidad desea puede generar más procedimientos si lo considera conveniente.

7. PRINCIPIOS DE AUDITORIA

La base de la auditoria, recae en los principios que sirven como lineamiento en el desarrollo de la misma, la cual permite proporcionar resultados confiables, objetivos, pertinentes y suficientes para que la organización pueda tomar las decisiones acerca de lo avanzado.

A continuación, se describen cada uno de los principios:

Integridad: El profesionalismo del auditor se debe llevar a cabo a partir de su honestidad, imparcial, diligencia y responsabilidad, demostrando su competencia durante el ejercicio de la auditoria.

Presentación ecuánime: El resultado de la auditoria (hallazgos, conclusiones e informes) deben reflejar la veracidad y exactitud de la información que se presentó durante el desarrollo de la auditoria.

Debido cuidado profesional: La habilidad del auditor en formular los juicios de valor razonables durante toda la auditoria.

Confidencialidad: La seguridad de la información, durante el ejercicio de la auditoria. Es un factor importante sobre el uso y la protección de la información, garantizando que no se utilice de manera inapropiada.

Independencia: La actuación del auditor se refleja en la independencia, libre de sesgo y conflicto de intereses. La independencia es la base de la imparcialidad y la objetividad del resultado de la auditoria, es así como está se mantiene objetiva durante todo el proceso.

Enfoque basado en la evidencia: El proceso de auditoria es una actividad sistemática, la cual se basa en la toma de muestras de la información por el tiempo limitado que se establece para una auditoria. Toda muestra debe permitir verificar la fiabilidad de la auditoria.

Al igual que los demás procedimientos planteados en el modelo de seguridad y privacidad de la información, se busca proteger la disponibilidad, integridad y confidencialidad de la información de la entidad.

8. FASES DE LA AUDITORIA

En el marco de la auditoria, está cuenta con 3 fases relacionadas a continuación:

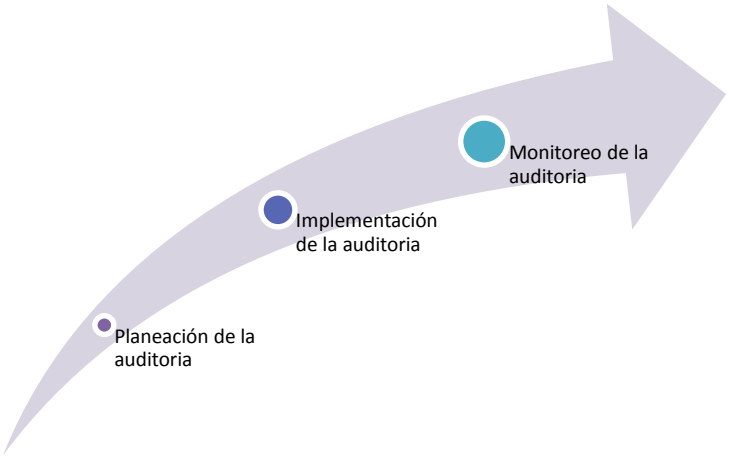

Imagen 1: Fases de la Auditoria

8.1. PLANEACIÓN DE LA AUDITORIA

Las auditorias se deben realizar al menos con una vez en el año, aunque esta periodicidad depende de las necesidades de la entidad. Durante la planeación se lleva a cabo el ciclo (planear) determinando los recursos, los procesos y el tiempo para llevar a cabo las auditorias, teniendo en cuenta como insumos las revisiones o seguimientos a la implementación del modelo de seguridad y privacidad de la información, observaciones por parte de la alta dirección, el desempeño de los procesos, los cambios en el entorno, controles internos, estrategias, entre otros.

Es importante que las auditorias se realicen con anterioridad a las auditorias de organismos de certificación y de control, con el fin de mejorar las deficiencias que pueda llegar a tener la implementación del modelo. También es necesario que los líderes de los procesos trabajen de forma alineada con el equipo de seguridad o la Oficina de Control Interno o la dependencia que haga sus veces, para determinar mesas de trabajo orientadas a revisar su proceso de manera que el trabajo se realice proactivamente y no reactivamente. Con lo anterior los resultados pueden

llegar a potencializar las acciones de mejora que agreguen valor a los procesos y por ende a la entidad.

La programación de la auditoria debe ser aprobada por la alta dirección y publicada en el sitio web, en la cual los líderes de los procesos conozcan las fechas y se preparen para recibir la auditoria.

8.2. IMPLEMENTACIÓN DE LA AUDITORIA

Durante esta fase, se prepara la auditoria. Inicia con la reunión de apertura, presentando la metodología, los tiempos y recursos que se utilizarán. Se recolecta y analiza la información evidenciando los hallazgos, las oportunidades de mejora y las fortalezas encontradas durante la auditoria. Una vez se culmine, se presenta durante la reunión de cierre las conclusiones de la auditoría.

Con base en el informe de la auditoria, se establecen las acciones de mejora pertinentes.

8.3. MONITOREO DE LA AUDITORIA

En esta última fase, se realiza el monitoreo al cumplimiento de las metas de las acciones: acciones correctivas, acciones preventivas o de mejora. La efectividad de las acciones permitirá la mejora de la implementación del modelo de seguridad y privacidad de la información. Es pertinente que el monitoreo se haga de forma permanente para hacer seguimiento de los avances e identificar cualquier acción que permita apalancar el cumplimiento de los objetivos.

9. AUDITORIA INFORMATICA

Es la actividad de recolectar, consolidar y evaluar evidencia para comprobar si la entidad ha avanzado en la implementación de controles, protección de los activos, mantenimiento de la integridad de los datos, si tiene claro los objetivos de seguridad de la entidad y si utiliza bien los recursos. De este modo la auditoría informática mantiene y confirma la consecución de los objetivos tradicionales de la auditoría, que son:

- Protección de activos e integridad de datos.
- Gestión de protección de activos, de manera eficaz y eficiente.

La auditoría Informática, puede ser externa como interna y debe ser una actividad ajena a influencias propias de la entidad. La función auditora puede actuar de oficio, por iniciativa o por solicitud de la dirección de la entidad.

10. AUDITORIA DE SISTEMAS

La auditoría de sistemas, es aquella actividad donde se evalúa el manejo y la protección de la información residente en los sistemas de información, también califica la aptitud del recurso humano que gestiona estas plataformas y la eficiencia del recurso informático.

La función de la auditoria es preventiva, realiza revisiones utilizando recursos de hardware y software desarrollando procedimientos similares a los que emplea la entidad, con el fin de mejorar los procesos de la entidad.

El objetivo principal es la verificación del sistema de información, su confiabilidad y el uso del mismo por parte de la entidad.

10.1. PERFIL DEL AUDITOR DE SISTEMAS

El Auditor es un asesor dentro de la entidad, su ubicación depende de la ubicación orgánica y funcional.

Se requieren calidades humanas, de gestor y de organizador, algunas de ellas:

- Eficiencia en su misión en la entidad.
- Ser diplomático.
- Manejo de pedagogía.
- Conocimiento de herramientas y métodos, para llegar al objetivo a alcanzar.
- Conocimiento en técnicas de auditoria.

11. METODOLOGIA DE LA AUDITORIA EN SISTEMAS

La metodología inicia con un proceso de planeación, en esta se fijan los objetivos y las herramientas a usar, esto implica que hacer, como hacerlo y cuando hacerlo.

Esta etapa incluye una investigación previa con el fin de conocer la operación de lo que se va a evaluar.

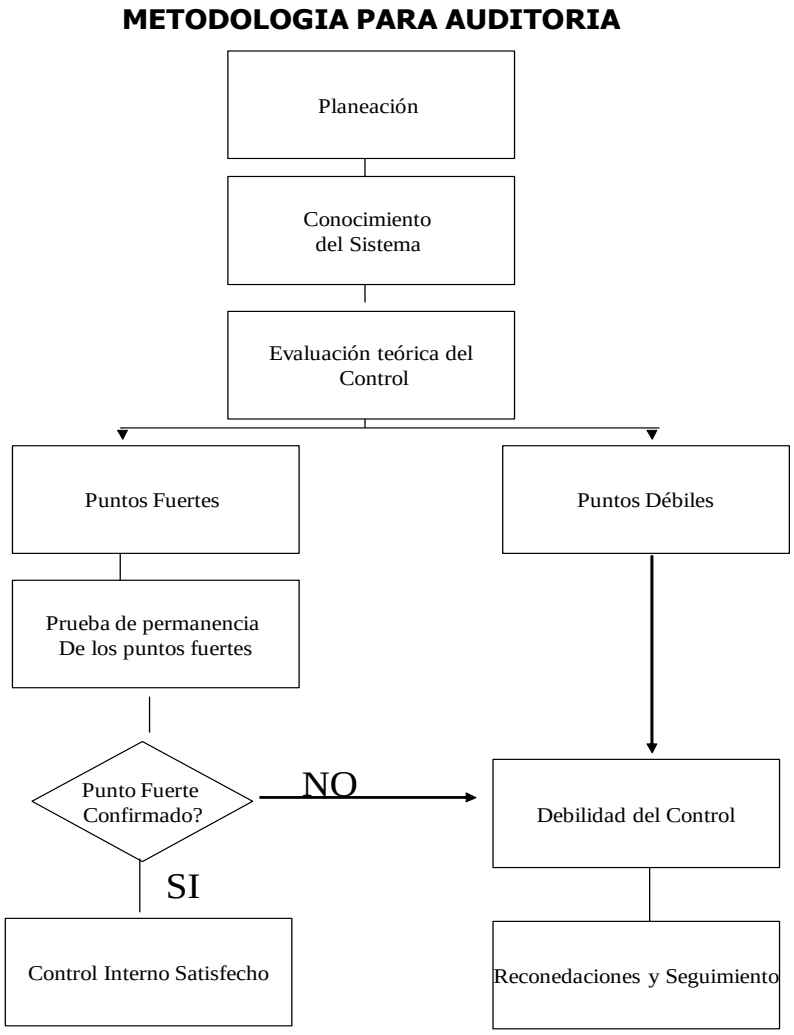

Figura 1: Metodología para Auditoria

12. METRICAS

Las métricas son medidas que nos proporcionan una medida cuantitativa de cantidad, dimensiones, capacidad, tamaño, de las propiedades de un proceso en la entidad.

Métrica: según el IEEE define la métrica como una medida cuantitativa del grado en que un sistema, componente o proceso posee un atributo dado.

El uso de las métricas, estas nos permiten entender un proceso técnico que se está aplicando en la entidad, a través de ellas podemos medir dicho proceso y su producto para saber cómo mejorar su calidad. La medición de los procesos es necesario para obtener un resultado de calidad que pueda llegar al ciudadano.

Todas las métricas que se pueden hacer para medir la calidad de un proceso y sus procesos de apoyo se agrupan en dos categorías diferentes dependiendo del tipo de métrica que se realice:

a) Métrica indirecta: en esta se centran en la calidad, complejidad, fiabilidad, eficiencia, funcionalidad, facilidad de mantenimiento, etc.

b) Métrica directa: respecto a esta se engloba en velocidad de ejecución, defectos encontrados en una cantidad de tiempo, costo, tamaño de memoria usada, número de líneas de código, etc.

12.1. MÉTRICAS DE SOFTWARE

Las métricas software se puede definir como “La aplicación continua de mediciones basadas en técnicas para el proceso de desarrollo del software y sus productos y servicios para suministrar información relevante a tiempo, así el administrador junto con el empleo de estas técnicas mejorará el proceso y sus productos”. Dichas métricas de software proveen la necesaria información para la toma de decisiones técnicas.

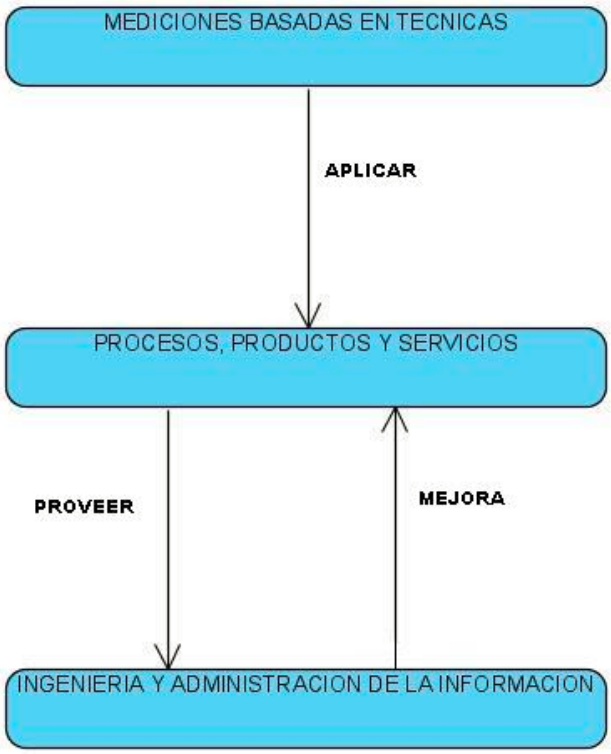

Imagen 2: Métricas

Las métricas sirven para realizar una medición de los sistemas de información, con el tiempo ayudan a mejorar el diseño y el análisis, mejorando con ello los procesos y resultados de los mismos.

Puntos clave de las métricas:

- No pueden ser ambiguas
- Deben tener estadísticas
- Deben automatizar la recolección de los datos

12.2. CREACIÓN DE UNA MÉTRICA

Para crear una métrica debemos de diseñar una tabla con toda la información correspondiente a dicha métrica, en la cual se indican todas las características que

posee que van desde su nombre, propósito, costo que tiene para la entidad, localización, tipo, etc.

12.3. MÉTRICAS DE SEGURIDAD

Son las mediciones de los procesos que determinan que tan bien se cumplen los procesos de seguridad en la entidad, si los procesos cumplen con los requisitos definidos por las políticas de seguridad y las normas técnicas seguidas por la entidad.

Estas evalúan el grado de riesgo de daño que pueden recibir objetos, recursos y personas. Contempla salud y seguridad tanto del usuario como de los afectados por dicho uso, al igual que consecuencias económicas o físicas no intencionadas.

Las métricas de seguridad se utilizan por:

- Gestión de seguridad de la información en la entidad.
- Proporcionar información para la gestión de informes.
- Indicar el cumplimiento de la legislación, reglamentación y las normas.
- Apoyo a las actividades de gestión de riesgos.

12.4. CARACTERÍSTICAS Y BENEFICIOS DE LAS MÉTRICAS DE SEGURIDAD

- Tienen que ser fáciles de obtener.
- Expresadas en porcentajes o números en escala.
- Necesarias con el fin de realizar tomas de decisiones.
- Tienen que ser detalladas explicando cada cosa que sea necesario.
- Encontrar posibles problemas que surgirán a corto plazo.
- Saber los puntos débiles de nuestra entidad.
- Conocer los riesgos que podemos obtener.

13. MEMSI – MODELO ESTRATEGICO DE METRICAS EN SEGURIDAD DE LA INFORMACION

El modelo estratégico de las métricas respecto a la seguridad de la información se divide en tres niveles.

a) Nivel estratégico

b) Nivel táctico

c) Nivel operativo.

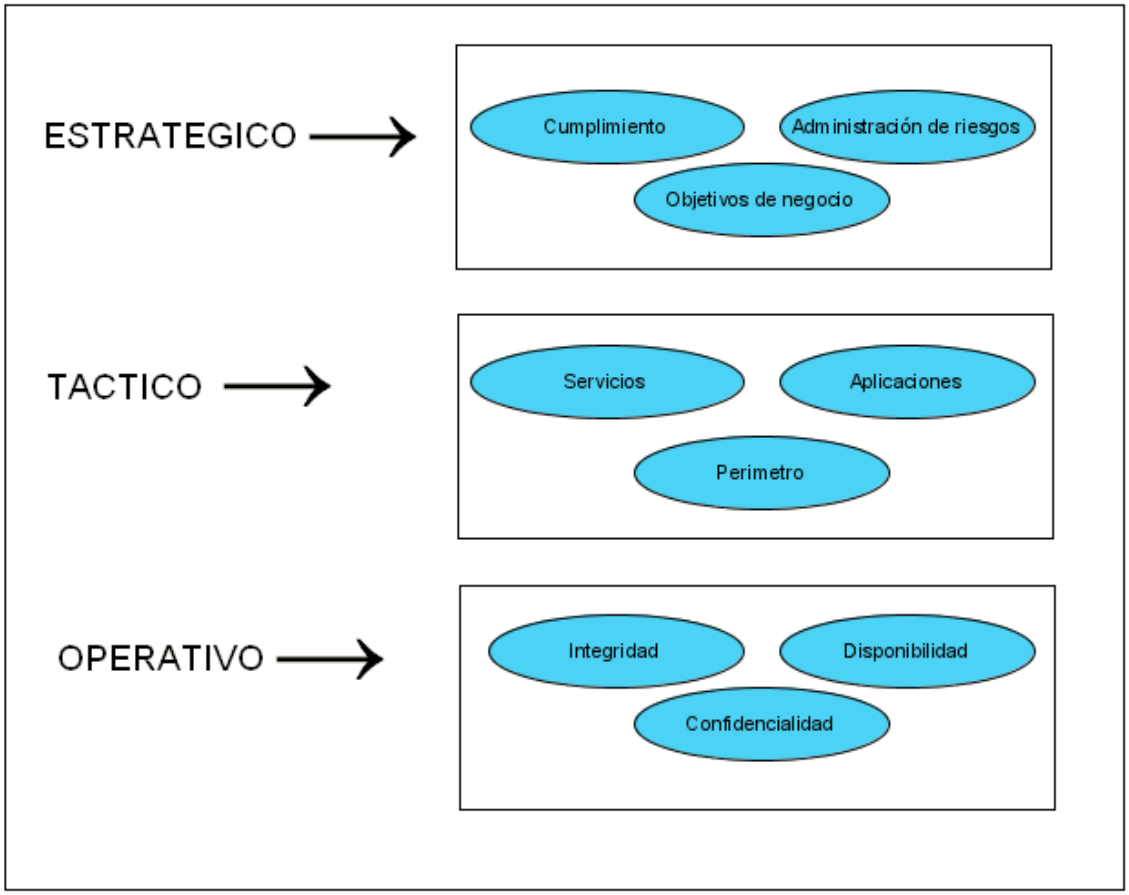

Imagen 3: MEMSI

a) En el nivel más alto conocido como nivel estratégico encontraremos tres grupos los cuales son:

- Cumplimiento: se centrará en llevar a cabo los estándares de la seguridad informática, realizar auditorías así como las pruebas de cumplimiento.
- Administración de riesgos: la cual consiste en identificación de los activos de la entidad a proteger, realizar ejercicios de análisis de controles y riesgos, realización de planes de seguimiento y actualización, creación de pruebas respecto a vulnerabilidades así como la creación de mapas de controles y riesgos.
- Objetivos de Negocio: este grupo se centrará en las relaciones con los usuarios o grupos de interés por parte de la entidad, la agilidad y responsabilidad ante incidentes que ocurran, el significado de la seguridad respecto a los procesos de la entidad y de las expectativas de la dirección en relación a la confianza de los sistemas.

b) En este nivel conocido como nivel táctico encontraremos otros tres grupos los cuales son:

- Servicios: el cual ser encarga del control de cambios, copias de respaldo, posibles recuperaciones ante fallos, el aseguramiento de equipos y la administración de parches.
- Aplicaciones: su responsabilidad es la siguiente, desde revisar el código fuente, defectos identificados en el software, pruebas de vulnerabilidad en software, vulnerabilidades identificadas y utilización de funciones no documentadas.
- Perímetro: este último se encarga de la efectividad de la seguridad que va desde la efectividad del Antispam, antivirus, firewall, así como la efectividad del monitoreo 24*7.

c) En el nivel conocido como nivel operativo encontraremos otros tres grupos los cuales son:

- Integridad: cuya función consiste en eliminar, borrar o manipular datos, como protegerse ante virus informáticos.
- Disponibilidad: se encarga de la negación del servicio, inundación de paquetes, suplantación de datos o IP, eliminar, borrar y manipular datos.
- Confidencialidad: este último debe estar preparado para encargarse desde contraseñas débiles, suplantación de IP o datos, accesos no autorizados por terceras personas, configuración por defecto que puede poner en peligro si no tiene la configuración deseada, monitoreo no autorizado.

7.1. EJEMPLOS DE MÉTRICAS PARA SEGURIDAD

Relacionaremos algunos ejemplos de métricas que podemos utilizar para alguno de los tres niveles que hemos comentado anteriormente, vale la pena mencionar que solo son algunos ejemplos y que pueden hacerse muchos más.

Nivel estratégico:

- Conocer el % (tanto por ciento) de las cuentas inactivas de usuario deshabilitadas respecto al total de cuentas inactivas.
- Conocer el valor total de los incidentes de seguridad informática respecto al presupuesto total de seguridad informática.
- Conocer el % (tanto por ciento) de los nuevos funcionarios que completaron su entrenamiento de seguridad respecto al total de los nuevos funcionarios que ingresaron.
- Propósito de esta métrica: desempeño de personas y procesos.

Nivel táctico:

- Conocer el número de mensajes salientes con spyware o virus.
- Numero de mensajes de spam detectado respecto al número total de mensajes ignorados.
- Número de estaciones de trabajo en funcionamiento configuradas correctamente respecto total de las estaciones de trabajo.
- Numero de spyware o virus detectados en estaciones de trabajo o servidores.
- Propósito de estas métricas: desempeño de las tecnologías de seguridad informática.

Nivel operativo:

- Número de incidentes asociados con la disponibilidad respecto al total de incidentes.
- Número de incidentes asociados con la confidencialidad respecto al total de incidentes.
- Propósito de estas métricas: desempeño de la administración de incidentes

El utilizar métricas de seguridad en el Sistema de Gestión de Seguridad de la Información puede provocar que la norma 27001 perdure en el tiempo como un estándar potente y eficaz para gestionar las seguridad de la información de una forma óptima, debido a que las métricas de seguridad no están contempladas como un accesorio más a añadir al Sistema de Gestión de Seguridad de la Información según le interese a la entidad sino que lo absorbe y termina formando parte de él a lo largo de su ciclo de vida. Todo esto provoca que el sistema de medición junto a su Sistema de Gestión de Seguridad de la Información sea revisado y mejorado de una forma continua.

7.2. MEDICIONES

La normativa ISO/IEC 27004 está centrada sobre el modelo Plan-Do-Check-Act, también conocido como PDCA, el cual consiste en un ciclo continuo.

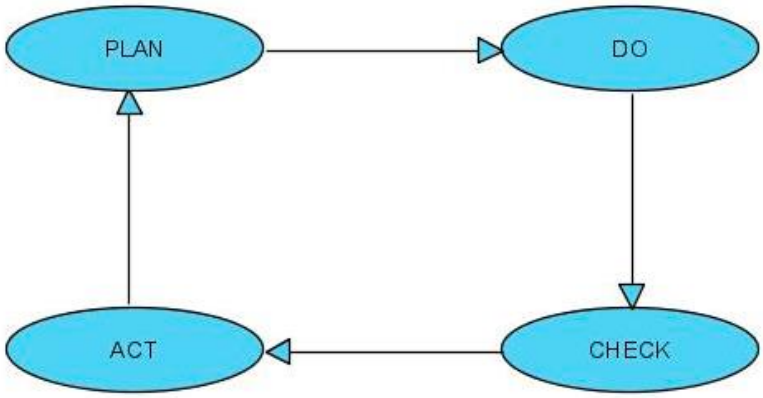

Imagen 4: Ciclo PDCA

La entidad debe saber cómo interactúan y se interrelacionan las mediciones de la entidad con su Sistema de Gestión de Seguridad de la Información. Para ello la entidad tendrá que crear una serie de guías las cuales especifiquen, señalen, documenten y expliquen estas relaciones con el máximo detalle posible con el fin de llevarlo a cabo lo mejor posible.

En los procesos de mediciones se tienen que cumplir una serie de objetivos los cuales son los siguientes.

- Indicar y avisar los valores de seguridad de la entidad.
- Realizar una evaluación de la eficiencia del Sistema de Gestión de Seguridad de la Información.
- Incluir niveles de seguridad que sirvan de guía para las revisiones del Sistema de Gestión de Seguridad de la Información, lo cual provocará nuevas entradas para auditar y para ayudar a mejorar la seguridad de la entidad.
- Realizar una evaluación de la efectividad de la implementación de los controles de la seguridad de la entidad.

7.3. MÉTODO DE LAS MEDICIONES

Esta normativa nos indica cómo los atributos tienen que ser medidos, por lo cual propone un Método.

Existen dos tipos de métodos a la hora de cuantificar los atributos necesarios.

Objetivos: los cuales se centran en una regla numérica (por ejemplo de 1 a 5) que se pueden aplicar a las personas o a los procesos, se recomienda que se realice primero a los procesos.

Subjetivos: se centran en el criterio de los empleados o de los evaluadores externos.

Dichos métodos pueden englobar diferentes tipos de actividades y a su vez un método engloba a varios atributos.

Algunos métodos que se utilizan en la entidad con el fin de medir los atributos son:

- Cuestionarios al personal de la entidad.
- Inspecciones de las aéreas de dicha organización.
- Toma de notas a partir de observaciones.
- Comparación de atributos en diferentes momentos.
- Muestreo.
- Consultas de los sistemas.

Una vez realizados los métodos de medición es asociarlo a un tipo de escala, las clases de escala pueden ser:

- Ratio: uso de escalas de distancias.
- Nominal: uso de valores categóricos
- Intervalos: uso de máximos y mínimos.
- Ordinal: uso de valores ordenados.

Al finalizar se tiene que considerar la frecuencia de cada medición. Se recomienda que la entidad programe dicha frecuencia de las mediciones, ya sean diarios, semanales, mensuales, semestrales, trimestrales, cuatrimestrales o anuales.

7.4. SELECCIÓN Y DEFINICIÓN DE LAS MEDICIONES

También se indica cómo desarrollar dichas mediciones para cuantificar la eficiencia de nuestro Sistema de Gestión de Seguridad de la Información, controles y procesos.

- Dichas mediciones de la información son requeridas para:
- La certificación de nuestro Sistema de Gestión de Seguridad de la Información de la entidad.
- La mejora en la eficiencia del Sistema de Gestión de Seguridad de la Información.
- Para los usuarios de la entidad, partes interesadas, etc.
- Para cumplir con las regulaciones y requisitos legales.
- Para la mejora de los procesos.
- Para la alta dirección de la entidad.

Ahora para poder realizar el establecimiento y la operación de un programa de mediciones necesita realizar los siguientes puntos en orden.

- Definir los procesos
- Desarrollo de mediciones
- Implementación del programa
- Revisión de mediciones.

Las mediciones pueden estar relacionadas con:

- Ejecución de controles de seguridad de la información, como puede ser por ejemplo el volumen de incidencias por tipo.
- Procesos de sistemas de gestión, como puede ser por ejemplo si se realizan las auditorías indicadas.
- Además las mediciones tienen que cumplir con una serie de criterios para que sean validadas por la entidad. Los cuales son:
- Cuantitativo: uso de datos numéricos.
- Indivisible: los datos de obtendrá en el nivel más bajo.
- Definición: tienen que estar bien documentadas de todas sus características (frecuencia, indicadores, etc.)
- Usable: los resultados sirven para la toma de decisiones.

- Verificable: las revisiones deben de ser capaz de valorar el dato y obtener resultados.
- Estratégico: tiene que estar en relación con la misión y la estrategia de la seguridad de la información.
- Razonable: el valor del dato obtenido no tiene que ser mayor al coste de recolectarlo.
- Tendencia: los datos deberían de ser representar el impacto cuando se realizan cambios.

A la hora de seleccionar los controles necesarios la entidad tiene que hacer los siguientes pasos:

- Definir un programa.
- Seleccionar los controles y objetivos de control para ser incluidos en dichas mediciones.
- Definir los indicadores para sus respectivos controles.

7.5. CUADRO DE GESTIÓN

Al cuadro de gestión se le considera como una de las herramientas más importantes, valiosas y potentes que puede utilizar la dirección de la entidad para evaluar su estado de seguridad el cual les servirá para la toma de decisiones.

Dicha herramienta deberá centrarse en los indicadores de la entidad; el objetivo principal del cuadro de gestión consistirá en mejorar los resultados que obtiene la entidad.

Para el seguimiento y la gestión de la información, se puede apoyar en el instrumento de diagnóstico y seguimiento que ha puesto a disposición de las entidades el Ministerio TIC.