MINISTERIO DE EDUCACIÓN, UNA REVISIÓN CRÍTICA DE SU POLÍTICA DE SEGURIDAD ACTUAL

Octubre 06 de 2010

LUIS GUILLERMO CAICEDO RAMOS
luis.guillermo.caicedo@gmail.com

Resumen

En el presente artículo se pretende dar las pautas pertinentes para saber de que forma se puede concientizar a las Personas que hacen parte directa o indirecta de todos los procesos que se manejan en el Ministerio de Educación referente a las Políticas de Seguridad de la Información; teniendo en cuenta el concepto, la aplicabilidad, la Tecnología, las normas, leyes, los medios y medidas para culturizar a toda la Organización en cuanto a este tema.

Abstract

In the present article the pertinent guidelines are tried to give to know of that form can concientizar to the Persons who do direct or indirect part of all the processes that they handle in the Department of Education relating to the Security policies of the Information; bearing in mind the concept, the applicability, the Technology, the procedure, laws, the means and measures for culturizar to the whole Organization as for this topic.

Palabras claves

Seguridad de la Información, Confidencialidad, Integridad, Disponibilidad, Sistema de Gestión de Seguridad de la Información, Incidentes de Seguridad.

Introducción

A lo largo de los últimos años se han incrementado los incidentes que hacen referencia al tema de Seguridad de la Información debido a la falta de conocimiento, las irresponsabilidades de cada individuo que hacen parte de los procesos y las pocas medidas que se toman para disminuir los riegos; es por ello que las Empresas u organizaciones a nivel mundial se están preocupando día tras día por minimizar los niveles de riesgo, analizar las vulnerabilidades y buscar nuevas alternativas para minimizar los ataques a las redes, Sistemas de Información y diversas plataformas tecnológicas. Estos ataques son transmitidos generalmente por medio de redes de comunicaciones, Internet, equipos, dispositivos, correos e Intranet, entre otros.

Gracias a las investigaciones realizadas, hoy día se puede decir que el tema de seguridad de la información no se debe basar exclusivamente a nivel tecnológico y es ahí donde radica el concepto erróneo de muchas empresas cuando se presentan problemas de seguridad, porque según la mayoría de las personas el problema fue causado por ejemplo, por un computador que se encontraba conectado a Internet y del cual se envío o se recibió un mensaje de correo que tenia un virus informático, el cual infectó todos los equipos que se encontraban conectados en la red corporativa; pero si se ahonda más en el tema, se podrá observar que pueden ser más críticos los procedimientos y funciones que se omiten, tal como dejar expuestos documentos importantes en el escritorio, para que cualquier persona haga uso indebido de la información que se encuentra allí; brindar información a terceros, la cual pueda ser utilizada por la competencia con fines no muy benéficos para la empresa y adicional a ello no se puede dejar de lado la información que esta circulando en la red tanto externa como interna de la Organización.

El objetivo principal del presente artículo es proporcionar a la dirección del MEN, la definición de políticas, procedimientos, guías y parámetros que se rigen de acuerdo a los requisitos, las normas y leyes que regulan los objetivos del negocio.

En la actualidad, el Ministerio de Educación Nacional, cuenta con una Política de Seguridad informática y es por ello que se debe desarrollar una revisión crítica de la política vigente para estructurar un mejor Sistema de Gestión de Seguridad de la Información al interior del MEN.

***Política de Seguridad Actual del MEN** [1]*

El documento de Política de Seguridad de la Información que se encuentra en el MEN, cuenta con 20 ítems, tales como: Seguridad para Servicios Informáticos, Seguridad para usuarios terceros, Seguridad Física y del entorno, Acceso a la Información, recursos informáticos, Software utilizado, Actualización de Hardware y Administración de la Seguridad, entre otros. Estos se presentan en el documento focalizados específicamente hacia el área de Tecnología, es por ello que a continuación se muestran algunas apreciaciones referentes a la Política de Seguridad actual en el MEN.

Críticas Formuladas de acuerdo a la Política de Seguridad Actual

De acuerdo a lo evidenciado en el documento de la Política de Seguridad de la Información, se formulan las siguientes críticas a la Política actual:

El documento fue desarrollado por la oficina de Tecnología y Sistemas de Información, en el cual no se cuenta en la mayoría de los casos con la opinión de otras áreas que deberían estar involucradas en las Políticas creadas; ya que se debe contar con un Gobierno Corporativo o mejor aún, con un Comité de Seguridad de la Información, el cual este integrado por la Junta Directiva del MEN, quien será la encargada de evaluar y modificar la política de acuerdo a los requerimientos y legislación vigente.

El nombre del documento que fue publicado en la Intranet de la siguiente manera "Políticas y Procedimientos para la Gestión de la Seguridad y la Conservación de la Información en el ministerio de educación" se encuentra bien definido, aunque en la introducción del documento, se inicia de inmediato con un error, debido a que se incluye específicamente el tema tecnológico en la siguiente frase "El proceso de gestión de la seguridad de tecnología de información y comunicaciones", lo cual da a entender que ya el documento esta basado en los parámetros tecnológicos; por consiguiente en el documento se debe buscar la focalización del Sistema de Gestión de Seguridad de la Información, en el que se comprenda el enfoque global de la información y a su vez se centre en todos los aspectos de los activos de información del MEN.

Las Políticas registradas en el documento hacen mucho hincapié a la Política de Seguridad Informática, conllevando con esto a que sean regidas por un solo proceso, en este caso solo el tecnológico, más no por varios procesos que se encaminen por lineamientos de verificación, gestión, clasificación y finalmente auditorias de los activos de información para ser controlados de la mejor forma posible, determinando así la creación de una Política de Seguridad de la Información bien cimentada y estructurada por la alta dirección del Ministerio de Educación. Además, en el ítem donde se expone la Administración de usuarios, no se tiene en cuenta la frecuencia con que los usuarios deben cambiar sus contraseñas y los períodos de vigencia de las mismas.

En el aparte que hace referencia a la Seguridad para los servicios informáticos se observa que la identificación de los controles de acceso se ejecutan de forma correcta, ya que existen restricciones a sitios de Internet, al uso indebido del correo corporativo, restricción de descargas de música, videos y sitios x, prohibición de archivos ejecutables que atenten contra la seguridad de la red a menos que pertenezcan al área de Tecnología y que estos tengan permisos especiales concedidos por los administradores de la red.

Sin embargo, en el momento en que un visitante se dirige a una de las oficinas de la entidad debe ser escoltado durante todo el tiempo por un empleado autorizado, asesor o contratista. Esto es algo que no se cumple por ninguno de los funcionarios del MEN.

“Los dueños de los recursos informáticos que no sean propiedad de la entidad y deban ser ubicados y administrados por ésta, deben garantizar la legalidad del recurso para su funcionamiento. Adicionalmente, debe definir un documento de acuerdo oficial entre las partes”. Por lo anterior se analiza y concluye que esto no se esta cumpliendo por parte del área responsable de verificar y velar por el cumplimiento de las políticas, en este caso la Oficina de Tecnología, ya que el Software en algunos casos no es licenciado.

Otro caso en donde se pasan por alto los procedimientos es en el siguiente aparte “Los equipos de usuarios terceros que deban estar conectados a la Red, deben cumplir con todas las normas de seguridad informática vigentes en la Entidad”. Según lo evidenciado por el personal de Mesa de

Ayuda es que en muchas de las áreas donde se manejan diversos proyectos, el personal contratado es por medio de Outsourcing o terceros que llevan sus propios equipos y van configurados de acuerdo a su Organización y en los cuales se detecta que en ocasiones van con virus o problemas que puedan afectar la Seguridad de los equipos que se encuentran interconectados en la red del MEN.

"Toda persona que se encuentre dentro de la entidad deberá portar su identificación en lugar visible". En la mayoría de los casos el personal tanto contratista como empleados del MEN no hacen uso del carné de identificación.

De acuerdo al objetivo expuesto "Garantizar que la información, como bien público, sea dispuesta a los funcionarios, usuarios y ciudadanos, según las necesidades del Sistema Integrado de Gestión de la Entidad, de manera que se pueda utilizar efectivamente, de forma segura y sin afectación a la calidad y confiabilidad de la misma", se concluye que la Información debe estar justo a tiempo para las personas que lo soliciten con el debido control de acceso y aplicando la integridad, confiabilidad y disponibilidad.

Comparación de la Política con estándares nacionales o internacionales *[2]*

La Política de Seguridad de la Información actual esta basada en algunos parámetros de la Norma ISO 27001:2005 en Gestión de Riesgos y también se basaron en aspectos regidos por la Norma ISO 9000 de Gestión de Calidad.

Propuesta de la nueva Política de Seguridad de la Información Para el MEN [3]

Alcance

La presente Política de Seguridad de la Información se encuentra estipulada dentro del cumplimiento de las normas legales vigentes, con el objetivo de realizar un adecuado Sistema de Gestión de Seguridad de la Información, diseñado para asegurar los controles suficientes y proporcionales que protejan los Activos de Información y brinden confianza a las partes interesadas, tales como: recurso de la Información, Organización de la Seguridad y el ámbito

tecnológico entre muchos otros aspectos que hacen parte de la Organización. El cumplimiento se debe dar a conocer y acatar por toda la planta de personal del Ministerio de Educación y el Personal externo que labore en la entidad estatal.

Objetivo

Administrar la seguridad de la información dentro del Ministerio de Educación, gestionando su implementación, así como la distribución de funciones y responsabilidades y a su vez divulgar a toda la Organización por medio de la Intranet, los procedimientos, deberes y responsabilidades en materia de seguridad de la información, de igual forma garantizando el cumplimiento de las Políticas de seguridad implementadas para funcionarios directos, personal de Outsourcing y/o terceros que tengan acceso a los Activos de Información dentro y fuera de las Instalaciones del MEN.

Responsabilidad

El Coordinador del Comité de Seguridad de la Información será el responsable de impulsar la implementación de la presente Política, al igual se encargará de la presentación para la aprobación de la misma ante la máxima autoridad del Ministerio de Educación, quien en este caso sería la Ministra de Educación y realizará el seguimiento de acuerdo a las incumbencias propias de cada área y de las actividades relativas a la seguridad de la información, conllevando con ello realizar un análisis de riesgos, implementación de controles, verificación de incidentes de seguridad, administración de gestión de continuidad, disponibilidad y concientización a todos y cada uno de los integrantes en los procesos que se llevan a cabo en el MEN.

Aspectos Generales

La Política de Seguridad esta compuesta por una serie de elementos que son de vital importancia para la Gestión de Seguridad de la Información del MEN, que incluyen los siguientes aspectos:

• ***Organización de la Seguridad:*** Se basa en la administración de la seguridad de la información dentro del MEN, estableciendo a su vez un marco gerencial para el control de su implementación.
• ***Clasificación y Control de Activos:*** Destinado a mantener una adecuada protección de los activos de Información de la Organización.

• ***Seguridad del Personal:*** Basado en la mitigación de los riesgos por parte del recurso humano, uso inadecuado de instalaciones, protección contra ilícitos.

• ***Seguridad Física y Ambiental:*** Controles de accesos no autorizados en las áreas físicas, daños e interferencia en las instalaciones o afectación y bloqueo de la información.

• ***Gestión de las Comunicaciones y las Operaciones:*** Propender por el funcionamiento adecuado y seguro de las instalaciones de procesamiento de la información y los medios de comunicación.

• ***Control de Acceso:*** Dirigido a controlar de forma correcta y segura el acceso lógico a la información sensible del MEN.

• ***Desarrollo y Mantenimiento de los Sistemas:*** Destinado a garantizar que se cumplan las medidas de seguridad pertinentes en los sistemas de Información desde el inicio del desarrollo, durante el mantenimiento y hasta su implementación.

• ***Administración de la Continuidad de las Actividades del Organismo:*** Dirigido a contrarrestar las interrupciones del servicio o de las actividades, protegiendo a su vez los procesos de mayor criticidad en el MEN y los efectos de problemas o fallas significativas ante desastres.

• ***Cumplimiento:*** El cumplimiento de la presente política, esta direccionada a impedir infracciones y violaciones de las leyes del derecho civil y penal; conforme a las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos y a los requisitos de seguridad. Con el fin de asegurar la implementación de los controles y medidas de seguridad comprendidas en el documento de Política de Seguridad de la Información del Ministerio de Educación, el Comité de Seguridad de la Información estará conformado por las Directivas del Ministerio y Jefes de Áreas, revisarán la presente Política, a efectos de mantenerla actualizada. Asimismo, efectuarán los cambios pertinentes dado el caso de modificaciones que sean necesarias en función a posibles cambios que puedan afectar su definición, como los cambios tecnológicos, variación de los controles e impacto de los incidentes de seguridad de la información.

Conclusiones

De acuerdo a lo evidenciado en el presente Artículo se puede llegar a la conclusión que la Política de Seguridad de la Información que esta estipulada en la actualidad en el Ministerio de Educación, presenta ciertas falencias en cuanto a su propósito final, en lo cual debe centrarse el

análisis y la mitigación de los riegos de los Activos de Información a nivel general y no solo tomando como punto de referencia la parte tecnológica de la Organización.

A pesar de que un gran número de organizaciones canalizan sus esfuerzos para definir directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, muy pocas alcanzan el éxito, ya que la primera barrera a la que se enfrentan es convencer a los altos directivos de la necesidad y beneficios de las políticas de seguridad de la información; pero gracias a la experticia que tiene la Ministra de Educación María Fernanda Campos en materia de Seguridad, se busca con ello actualizar y ajustar los procedimientos recomendados para una buena Gestión de Seguridad aplicándola de acuerdo a la implementación de Políticas de Seguridad de la Información y basado en la norma ISO 27001 y estándares a nivel internacional para que ayuden al mejoramiento continuo de la Organización, poniendo en alto el buen nombre del Ministerio frente a otras entidades gubernamentales y a su vez desarrollando cultura de seguridad de la información para todos y cada uno de los integrantes que hacen parte del Ministerio de Educación Nacional.

Referencias Bibliográficas

[1] Briceño Andrés, Políticas Y Procedimientos Para La Gestión de La Seguridad y La Conservación de La Información en el Ministerio de Educación, Documento de Políticas de Seguridad Informática, Versión 2, Marzo 2009.

[2] Piattini M., Del Peso E., Auditoría de la Seguridad Un enfoque práctico, Evaluación de Riesgos y Auditoría de Gestión de Calidad, Alfa Omega Grupo Editor, 2005.

[3] Achiary C., Modelo de Política de Seguridad de la Información, Política Modelo, Versión 1, http://www.arcert.gov.ar/politica/PSI_Modelo-v1_200507.pdf, Julio 2005.