



Ministerio de Educación
Dirección de Auditoría Interna
Gerencia de Auditoría Educativa y Administrativa

MINISTERIO DE EDUCACIÓN
GOBIERNO DE
EL SALVADOR
UNÁMONOS PARA CRECER

Enfoque de Auditoría: "Creación de Valor" y "Administración de Riesgo"

Unidad Organizativa Auditada: Dirección de Planificación (DP), Gerencia de Tecnologías de Información y Comunicación

VERSIÓN PÚBLICA - Art. 30 y Art. 6 Lit. "A" de la Ley de Acceso a la Información Pública (LAIP), referente a la supresión de datos personales.

INFORME FINAL DE AUDITORÍA INTERNA

Ref. MINED/DAI/GAEA/NA-057/2016

Auditoría de Examen Especial, de Tipo de gestión al Soporte de Licenciamiento del Software de Seguridad, correspondiente del 01 enero de 2015 al 31 de octubre de 2016 y actualizado a mayo 2017.

Versión Pública

San Salvador, mayo de 2017

MISIÓN DE LA DIRECCIÓN DE AUDITORÍA INTERNA: Somos un Equipo que proveemos servicios de Aseguramiento y Consultoría de forma independiente y objetiva, mediante un enfoque sistemático y disciplinado, evaluando y promoviendo la mejora de los procesos claves del control interno del Ministerio de Educación.

VISIÓN DE LA DIRECCIÓN DE AUDITORÍA INTERNA: Ser un equipo de profesionales que aplique estándares internacionales de auditoría interna; coadyuvando a la mejora de la calidad educativa.

... "Tres ejes transversales del Nuevo Modelo Educativo: la Ciencia y la Tecnología, el arte y la cultura y la recreación y Deporte."...

Alameda Juan Pablo II, intersección Calle Guadalupe, Plan Maestro Edificio A-2 segunda planta, Centro de Gobierno, San Salvador, Tel. 2592-2225

Email: direcciondeauditoriainterna@mined.gob.sv



DESTINATARIOS – LISTA DE DISTRIBUCIÓN:

Dirigido a Titular y Unidad Organizativa Auditada:

- Ministro de Educación ^(1/)^(3/)
- Director de Planificación ^(2/)^(3/)
- Directora de Contrataciones Institucionales ^(2/)^(3/)

Responsables del Sistema de Control Interno:

- Gerencia de Tecnologías de Información y Comunicación (GTIC) ^(2/)^(3/)
- Gerente de Adquisiciones y Contrataciones Institucional ^(2/)^(3/)

Funcionario, empleados y/o terceros relacionados:

- Corte de Cuentas de la República, Dirección de Auditoría Cuatro ^(1/)^(3/)

^(1/) Informe de Auditoría Notificado [Art.37 Ley de la Corte de Cuentas de la República] y [Art.202 Normas de Auditoría Interna del Sector Gubernamental]

^(2/) Informe de Auditoría Notificado [Art.202 Normas de Auditoría Interna del Sector Gubernamental] y comunicado [Art.5 Normas Técnicas de Control Interno Especificas del MINED]

^(3/) Informe de Auditoría entregado vía electrónica



ÍNDICE

| | |
|---|-----------|
| I. INTRODUCCIÓN..... | 4 |
| II. OBJETIVOS DE LA AUDITORIA..... | 5 |
| III. ALCANCE DE LA AUDITORIA..... | 5 |
| IV. PROCEDIMIENTOS DE AUDITORÍA APLICADOS..... | 5 |
| V. RESULTADOS DE LA AUDITORIA..... | 6 |
| VI. OBSERVACIONES DE AUDITORIA..... | 12 |
| HA-1: FALTA DE CONTROL EN LA IMPLEMENTACIÓN Y ACTUALIZACIÓN DE LOS SISTEMAS DE SEGURIDAD..... | 12 |
| HA-2: PROCESO TARDÍO DE CONTRATACIÓN DE LICENCIAMIENTO DE LOS SISTEMAS DE SEGURIDAD INFORMÁTICA..... | 16 |
| VII. RECOMENDACIONES..... | 18 |
| VIII. SEGUIMIENTO DE AUDITORÍA..... | 18 |
| IX. CONCLUSIÓN DE LA AUDITORIA..... | 18 |
| X. PÁRRAFO ACLARATORIO..... | 19 |
| XI. AGRADECIMIENTOS..... | 19 |
| XII. LUGAR Y FECHA..... | 19 |
| XIII. FIRMA DEL RESPONSABLE DE LA DIRECCION DE AUDITORIA INTERNA..... | 19 |

Versión Pública



I. INTRODUCCIÓN

La presente auditoría por examen especial de tipo de gestión al Soporte de Licenciamiento del Software de Seguridad, fue realizada según el plan de trabajo 2016 de la Dirección de Auditoría Interna (DAI).

La infraestructura de seguridad interna y externa del MINED, que cubre las principales áreas de riesgo tales como: Telecomunicaciones, servidores de sistemas operativos, bases de datos, aplicaciones internas y de terceros (Ministerio de Hacienda), sistemas biométricos y seguridad física institucional. El inventario total que incluye el sistema de licenciamiento en seguridad es de 6,186 recursos tecnológicos y datos de los sistemas de información, distribuidos en: 114 servidores, 131 equipos de comunicación, 1,809 estaciones de trabajo, 28 equipos biométricos, 6 equipos de seguridad 4,098 usuarios de red y correo electrónico; asimismo, soporta 12,585 licencias de software entre libre y patentado.

En **cuadro No. 1**, se detallan los montos ejecutados y a ejecutarse en la adquisición del Licenciamiento de Software de Seguridad.

Cuadro No. 1

Empresas Adjudicadas para proporcionar Licenciamiento de Software de Seguridad

| Empresa Contratada | Montos Desembolsados 2015 | Montos a Ejecutarse 2016 |
|---------------------------|----------------------------------|---------------------------------|
| | US\$11,300.00 | US\$0.00 |
| | US\$211,184.95 | US\$0.00 |
| | US\$0.00 | US\$56,528.76 |
| | US\$0.00 | US\$128,736.58 |
| Totales | US\$222,484.95 | US\$185,265.34 |

Los montos detallados para el año 2015 y 2016 para dar soporte de seguridad, incluyen:

- La empresa [REDACTED] con un monto US\$11,300.00, para administración de la plataforma de publicación de aplicaciones web.
- La empresa [REDACTED] con un monto de US\$211,184.95, fue adjudicado en dos ítems. El primero para licenciamiento de plataforma de servidores Microsoft por un monto US\$65,638.38, y el segundo para el licenciamiento del área seguridad con un monto de US\$145,546.57.
- La empresa [REDACTED] con un monto US\$56,520.83, fue adjudicada para licenciamiento de plataforma de servidores Microsoft.



II. OBJETIVOS DE LA AUDITORIA

General:

Medir la efectividad del Proceso de Contratación y Soporte del Licenciamiento del Software de Seguridad Informática.

Específicos:

- 1) Establecer la efectividad del proceso de contratación del Software de Seguridad,
- 2) Validar la seguridad institucional y efectividad de las políticas implementadas,

III. ALCANCE DE LA AUDITORIA

Periodo: Del 01 de enero de 2015 al 31 de octubre de 2016.

La auditoría se realizó de conformidad con las Normas de Auditoría Interna del Sector Gubernamental (NAIG), emitidas por la Corte de Cuentas de la República, en lo aplicable.

La auditoría se realizó conforme al marco de control interno adoptado por el Ministerio de Educación, conocido como Normas Técnicas de Control Interno Específicas (NTCIE), con enfoque COSO autorizadas por la Corte de Cuentas de la República, vigentes a partir del 28 de noviembre de 2013 a la fecha; la Ley de Adquisiciones y Contrataciones de la Administración Pública y su Reglamento para evaluar el proceso de compra.

Aspectos Evaluados:

Entre los aspectos evaluados, están:

1. Evaluación del Control Interno.
2. Efectividad e Implementación del Sistema de Seguridad Informático.
3. Cumplimiento Legal.

IV. PROCEDIMIENTOS DE AUDITORÍA APLICADOS

Entre los procedimientos de auditoría realizados, están:

1. Verificación del Sistema de Control Interno y la aplicación de las políticas de seguridad institucional.
2. Análisis del proceso de compra de contratación de las Licencias de Software.



V. RESULTADOS DE LA AUDITORIA

V.1) EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO Y APLICACIÓN DE LOS SISTEMAS DE SEGURIDAD INFORMÁTICOS.

Al evaluar el ambiente de control vigente para la seguridad informática del MINED, comprobamos la existencia de las siguientes debilidades de control:

- a) No existen Estándares de Seguridad de Tecnologías de Información y Documento de Arquitectura de Información del MINED, ya que no ha sido elaborado por la Gerencia de Tecnologías de Información y Comunicación. Dichos estándares deben establecer las medidas y patrones técnicos de administración y monitoreo de las políticas de seguridad institucional; así como las sanciones a los usuarios de incumplimiento de las políticas y la cobertura de los Riesgos contemplados en la Ley Especial contra los delitos informáticos y conexos, publicada en Diario Oficial No. 40 Tomo 410 de Febrero 2016.

De igual forma, la Arquitectura de Información del MINED debe establecer en forma específica el diseño, organización y distribución de los Sistemas de Información, su relación con la Ley de Acceso a la Información Pública y las especificaciones de las bases de datos y dueños de la información. **Ver detalle en Hallazgo HA-1.**

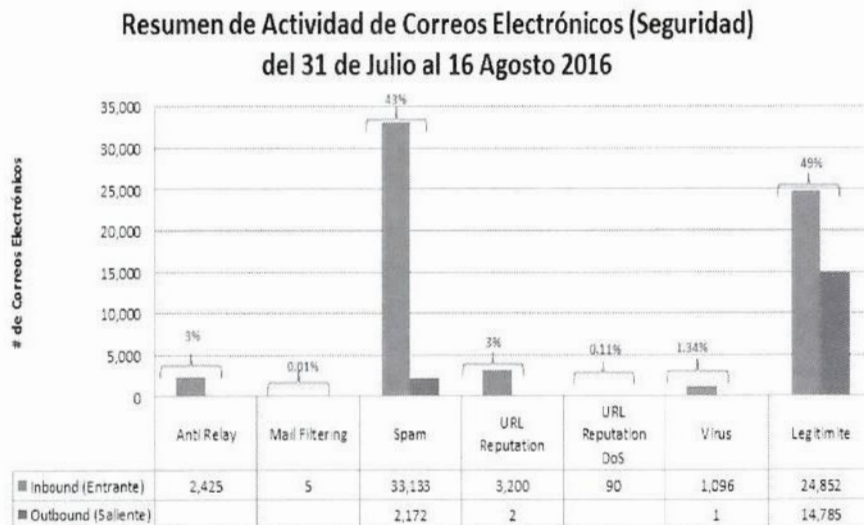
- b) El Plan de Contingencias de las Tecnologías de Información y la Metodología para la Identificación de los Riesgos Informáticos; no han sido, gestionado para autorización del Comité Estratégico de Tecnologías de Información (CETI), lo cual, deja sin ningún efecto legal y administrativo su aplicación.
- c) Actualmente la administración de la seguridad institucional, descansa en la Jefatura de Infraestructura Tecnológica y la Gerencia de Tecnologías de Información y Comunicación (GTIC), adscritas a la Dirección de Planificación y es administrada por un técnico administrador de la seguridad, quien coordina con las diferentes jefaturas de la GTIC los accesos y permisos de red correspondientes; sin embargo, este no realiza monitoreo del área y no presenta reportes de la efectividad de las políticas implementadas.



Lo anterior, genera una falta de segregación de funciones, dado que el Administrador de la seguridad concentra todas las funciones del proceso (diseña, implementa, modifica, elimina, monitorea y reporta); generando el riesgo de que:

- 1) El Administrador de la Seguridad, aplique de manera conveniente a su línea jerárquica, las políticas de seguridad.
 - 2) Las inversiones en el rubro de seguridad, se vean recortadas, de conformidad a las prioridades de la Dirección de Planificación.
 - 3) No se mida correctamente la efectividad de las políticas de seguridad implementadas.
- d) El MINED no cuenta con herramientas que permitan monitorear el grado de efectividad de las políticas de seguridad implementadas y generación de información gerencial, para la toma de decisiones importantes en este rubro, únicamente se cuenta con el reportería básica de las soluciones primarias: a) Filtro del correo electrónico (SMTP), b) Filtro Web, c) IPS (Sistema de Prevención de Intrusos), d) Firewall y e) Antivirus; no obstante, dichos reportes, nos permiten concluir sobre las tendencias siguientes:
- i. Filtro de correo electrónico. Se tiene un total de 1,500 reglas para filtrado de correos electrónicos entrantes, con el objeto de bloquear el contenido malicioso (entrantes y salientes); a manera de muestra, se analizó, el comportamiento de la efectividad de las reglas, en el periodo comprendido del 31 de julio al 16 de agosto de 2016. En gráfico No. 1 se muestra comportamiento.

Gráfico No. 1



Fuente: Reportes Semanales de la Consola de Administración de Seguridad

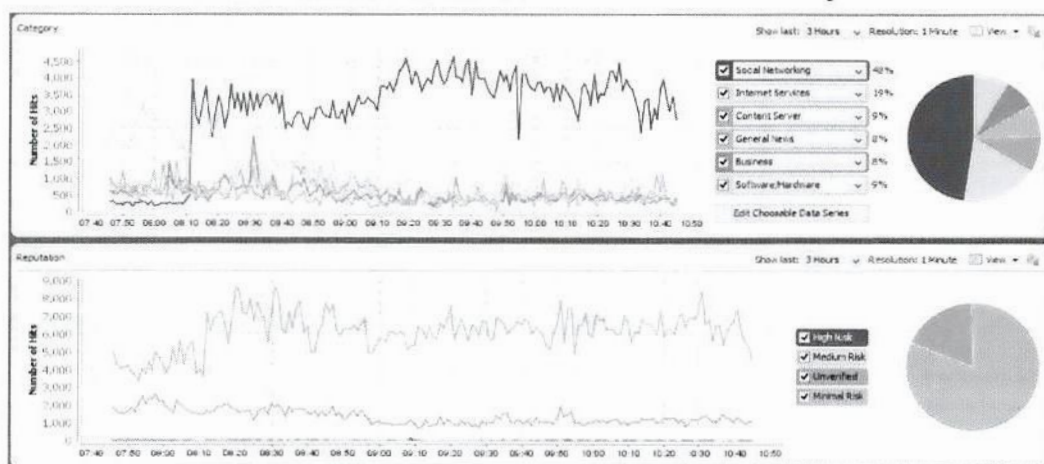


Como puede observarse en la gráfica, ingresan a los buzones de correo electrónico institucionales un promedio de 64,801 correos quincenalmente, de los cuales el 51% representa amenazas, las cuales fueron bloqueadas bajo diferentes conceptos, sobresaliendo el Spam y el 49% representado por correos validos que cumplen con todas las reglas de seguridad.

Caso contrario sucede en los correos enviados desde buzones institucionales de los cuales, solo un 15% corresponde a envío de spam; sin embargo, pudimos comprobar en 2 buzones de correo electrónico ([REDACTED]), que a pesar de las reglas de bloqueo de Spam, están ingresando un promedio de 8 correos con spam diarios a los buzones antes descritos, con una tendencia incremental de un 300% en el ingreso de spam, ocasionado principalmente por la falta de licenciamiento del software de seguridad (2 spam diarios con licenciamiento vrs 8 diarios con licenciamiento caducado).

- ii. Filtro Web. Se han implementado 700 reglas para filtrado Web, con el objeto de proveer protección y monitoreo de los sitios web públicos y privados que poseen contenido malicioso, mediante la herramienta de McAfee WG5500 (actualmente sin soporte por el proveedor). Este filtrado soporta alrededor de 1,000 usuarios a nivel nacional y un promedio diario de 816,000 solicitudes web; observándose según las estadística del filtrado de la aplicación que el 48% de la navegación es a las redes sociales y un 19% a sitios web de servicios de internet (clasificaciones provenientes del sitio web visitado).

Gráfico No. 2 – Monitoreo de los Sitios Web Públicos y Privados



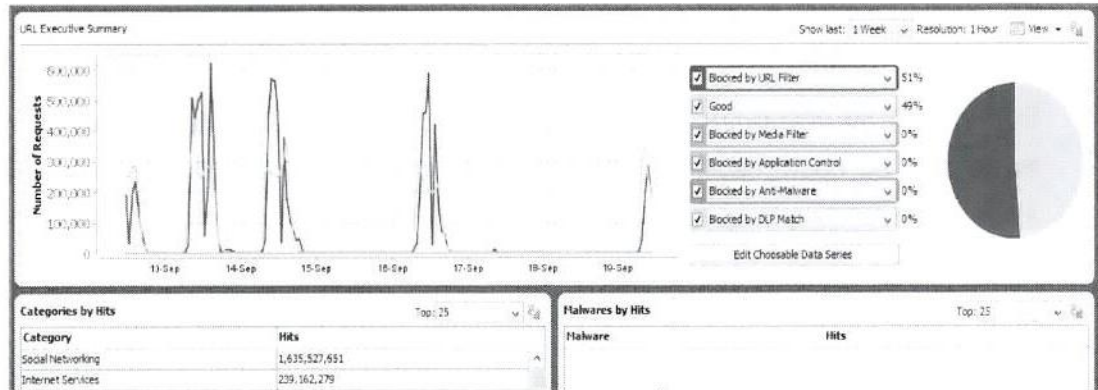
Fuente: Estadística emitida por el Software de Filtrado Web



Adicionalmente, se analizaron los bloqueos de la navegación hechas por el software en la semana del 13 al 19 de septiembre 2016, por el tipo de bloqueo web, identificado que existe una estadística del 51% de sitios bloqueados y solo un 49% de sitios permitidos; lo que indica una marcada tendencia de los usuarios hacia sitios no permitidos.

Grafica No. 3

Comportamiento de los usuarios a sitios bloqueado y no permitidos



Fuente: Estadística emitida por el Software de Filtrado Web

- iii. IPS (Sistema de Prevención de Intrusos). Existen 16,254 políticas de seguridad (sugeridas por la base de datos global de McAfee), las cuales se basan en el contenido del tráfico externo que entra a la red institucional, manejando 4 clases de severidad del ataque (altos, medios, bajos e informacionales) y dos tipos de eventos (Alertas y Ataques).

En cuadro No. 2, se visualiza un resumen de la contabilización para el primer semestre de 2016 y la cantidad de 5,425,665 ataques y 474,838 alertas de seguridad, bajo diferentes categorías.

Cuadro No. 2

Contabilización de ataques cibernéticos y alertas de seguridad

| # | Severidad de Ataque | Cantidad de Ataques |
|--------------|---------------------|---------------------|
| 1 | Alto | 12,952 |
| 2 | Medio | 116,628 |
| 3 | Bajo | 55,557 |
| 4 | Informacional | 5,240,528 |
| TOTAL | | 5,425,665 |



Versión Pública

Para el período contabilizado, de Julio a Septiembre de 2016 se reflejaron 26,878,098 ataques y 1,788,881 alertas de seguridad; lo cual, revela que los atacantes están informados que no contamos con actualizaciones del sistema de seguridad. Dado que, los ataques se han incrementado en un 395% y proporcionalmente las alarmas en un 277% entre julio y septiembre de 2016. Esta situación crea una alarma de riesgo **ALTO** puesto que no estamos preparados contra las nuevas formas de penetración y ataque a nuestros servidores institucionales.

El MINED cuenta con 3 dispositivos IPS Intrushield 2750 (hardware), de los cuales únicamente se encuentra en uso 1 de ellos, por falta de presupuesto para la compra de las interfaces; su costo oscila en US\$2,000.00 cada una y cada dispositivo cuenta con 10 de ellas; este hardware es, administrado por un software de McAfee propietario, el cual a la fecha no cuenta con licencia para soporte (venció en junio 2016); impactando, en la falta de obtención de reportes que ayuden a la administración de la seguridad.

La falta de este tipo de reportes, genera que la Dirección del MINED no cuente con información importante para medir el grado de efectividad de las políticas de seguridad y que las mismas no sean suficientes para evitar el hurto, accesos no autorizados, daños, etc., de la información institucional; así como, no ayuda a la toma de decisiones por la falta de comunicación de ello al CETI y que puede además, llevar hasta el congelamiento de los fondos presupuestados, por inicio tardío de los procesos de adquisición.

V.2) PROCESO DE CONTRATACIÓN DE LAS LICENCIAS DE SOFTWARE.

Respecto a los recursos de seguridad citados en el Romano V.1, ninguno cuenta con herramientas de reportes que le permitan un análisis gerencial y que este sirva de insumo para mejorar las políticas de seguridad actuales. Lo anterior, es ocasionado por la falta de licenciamiento de los productos (software) de seguridad, los cuales caducaron en junio de 2016 y la Gerencia de Tecnologías de Información y Comunicación (GTIC), inicio tardíamente el proceso de contratación de los mismos para 2016; a la fecha, según la Dirección de Contrataciones Institucionales, se encuentra pendiente de emitir la orden de inicio. **Ver detalle en Hallazgo HA-2.**

Por lo antes expuesto, la Gerencia de Tecnologías de Información y Comunicación (GTIC); por medio de, la Jefatura de Arquitectura Tecnológica, ha considerado la creación de 6 áreas para la implementación de las políticas de seguridad como se muestra en Cuadro No. 3.



Cuadro No. 3

Áreas identificadas para la implementación de políticas de seguridad

| Área de Protección | Descripción | Protegidos |
|--|--|---|
| Autenticación de Usuarios | Creación de credenciales que permiten la autenticación de usuarios y uso de los recursos y servicios institucionales. | 4,098 Usuarios |
| Creación de VLAN's | Para evitar las propagaciones de virus u otras amenazas entre múltiples subredes y ocurra un exagerado consumo de recursos, no intencional o causar denegaciones de servicio. | 38 Redes Virtuales |
| Acceso a Internet | Para suministrar el servicio de acceso a Internet se utiliza el filtrado web configurado como Proxy Server, permitiendo una conexión segura hacia internet, con grupos de trabajo. | 1,000,000 Sitios Web (promedio visitados semanalmente) |
| Protección por segmento de red (IPS/IDS). | Permite detectar accesos no autorizados, software maliciosos, tráfico innecesario, modificaciones en sistemas. | Promedio: <ul style="list-style-type: none"> • 55,955 correos semanales • 1,500 reglas de seguridad • 3,099 ataques diarios a los servidores MINED |
| Protección Anti-Spam | Prevención de virus, spam, solicitudes SMTP a servidores. | |
| Seguridad perimetral | Firewall para filtrado de accesos a la información y Antivirus. | |

Versión Pública



VI. OBSERVACIONES DE AUDITORIA

HA-1: FALTA DE CONTROL EN LA IMPLEMENTACIÓN Y ACTUALIZACIÓN DE LOS SISTEMAS DE SEGURIDAD.

| | |
|-----------------------------|---------------------|
| Importancia del Hallazgo: | Riesgo Medio |
| Componente NTCIE impactado: | Ambiente de Control |

Observación:

Al evaluar el funcionamiento del sistema de control interno del área de Informática, comprobamos que no existen Estándares de Seguridad de Tecnologías de Información; así como, documentos de la Arquitectura de Información del MINED y planes de contingencias e identificación de riesgos informáticos; debido a que, la Gerencia de Tecnologías de Información y Comunicación, durante la auditoría ha realizado el borrador de la Arquitectura de Información y será gestionada su aprobación ante el Comité Estratégico de Tecnologías de Información (CETI) durante el primer semestre del 2017.

Dichos Estándares de Seguridad de Tecnologías de Información, deben establecer las medidas y patrones técnicos de administración y monitoreo de las políticas de seguridad institucional; así como, las sanciones y la cobertura de los Riesgos contemplados en la Ley Especial contra los delitos informáticos y conexos, publicada en Diario Oficial No. 40 Tomo 410 de Febrero 2016. De igual forma, la Arquitectura de Información del MINED debe establecer en forma específica el diseño, organización y distribución de los Sistemas de Información, su relación con la Ley de Acceso a la Información Pública y las especificaciones de las bases de datos y dueños de la información.

Respecto al Plan de Contingencias de las Tecnologías de Información y la Metodología, en Cuadro No. 4 se detalla la Identificación de los Riesgos Informáticos actuales.

Cuadro No. 4 – Identificación de Riesgos Informáticos

| Nombre del documento | Contenido del documento | Estado actual |
|---|--|--|
| Plan de Contingencias de las Tecnologías de Información. | Reanudar el inicio de las operaciones de las TI, para el MINED en el caso de que ocurra una falla total del Centro de Datos y así lograr una exitosa recuperación de los servicios críticos de TI. | Se actualizo por última vez en 2013 y fue autorizado por el Viceministro de ese año. |
| Metodología para la identificación de los Riesgos Informáticos. | Metodologías y pasos a seguir para ejecutar una identificación de riesgos de TI efectiva en las oficinas centrales y Departamentales. | Actualizado en 2014. |



Al evaluar, el Plan de Contingencias de las Tecnologías de información, se identificaron las siguientes debilidades:

- No existen evidencias que se hayan ejecutado las pruebas que garanticen el grado de efectividad para su implementación y desarrollo.
- La información contenida en el mismo, a la fecha, ya se encuentra desactualizada con los nuevos recursos, proveedores y estructura de funcionamiento de la Gerencia de Tecnologías de Información y Comunicación.

Por otra parte, observamos que no existe una matriz de riesgos informático creada por la Gerencia de Tecnologías de Información y Comunicación que permita identificar y medir toda la posibilidad de ataques cibernéticos que pudiese sufrir el MINED; así como, las medidas necesarias para contrarrestas cada uno.

Normativa incumplida:

Normas Técnicas de Control Interno Especificas para el MINED, Definición de Políticas y Procedimientos de Controles Generales de los Sistemas de Información, Art. 323.-

“Para las operaciones relacionadas a las tecnologías de información, las unidades de Informática elaborarán documentos de soporte, según la siguiente distribución de responsabilidades: a) Todas las Unidades Proveedoras de Servicios de Tecnologías de Información: Portafolio de Proyectos y Servicios; Catálogo de Servicio Basado en Tecnología de Información; y Manual de Procedimientos; b) Gerencia de Informática: Plan de Infraestructura Tecnológica, del Ministerio de Educación; Plan de Adquisiciones de Infraestructura Tecnológica; Plan de Contingencia de las Tecnologías de Información; Plan de Mantenimiento de la Infraestructura Tecnológica; y Estándares de Seguridad de Tecnologías de Información.

El Comité Estratégico de Tecnologías de la Información (CETI), autorizará los documentos antes mencionados y cualquier otro documento realizado, relacionado a las tecnologías de la información”.

Causa:

- Falta de elaboración de Planes de Contingencia; Estándares de Seguridad de Tecnologías de Información; Arquitectura de Información del MINED, por la GTIC.



Efectos:

- Administración de la seguridad institucional de forma discrecional o a conveniencia de terceros, por no contar con un marco regulatorio.
- Políticas de seguridad institucionales implementadas que no cubran los delitos tipificados en la Ley especial contra delitos informáticos.
- Falta de deducción de responsabilidades en casos de fraudes o situaciones que ocasionen detrimento patrimonial, pérdida de imagen, entre otros por personal interno y externo del MINED,
- Vulnerabilidades y exposición a los riesgos de TI y que las decisiones de inversión en hardware o software de mayor envergadura, se direccionen erróneamente.

Comentarios de la Administración (Gerencia de Informática):

En atención a las observaciones establecidas, la Gerencia de informática presentó los siguientes comentarios y documentos relacionados: *“La infraestructura de Tecnologías de Información del Ministerio de Educación trabaja bajo políticas y estándares que permiten controlar el acceso de los usuarios institucionales, también de publicar externamente todas las aplicaciones y sitios web, lo que demuestra la existencia de estándares de seguridad. Esto se puede evaluar en los siguientes documentos:*

1. *MAN-DIT-001+Manual+de+procedimientos+-+Depto+de+Infraestructura+Tecnologica+V0.4+al+04-01-2012.pdf*
2. *DetallePolíticasSeguridadImplementadas-V1.doc*
3. *Estructura de las Políticas de seguridad institucional-Entorno-Fisico.doc*

Además se está elaborando un documento para consolidar las políticas, el cual estará listo en 2017...

En referencia a las sanciones de los usuarios de incumplimiento de políticas esta Gerencia de GTICs, no puede establecer sanciones que están definidas por la ley del servicio civiles y las normativas de la Direccion de Desarrollo Humano, ya que el mal uso de las TI, como cualquier otro recurso del Ministerio de Educación, debe establecerse por sanciones que sean consecuencias del proceso legal pertinente contra los empleados”. Además:

- *Se revisarán los planes detallados en el cuadro No. 5 en este año.*
- *Se han ejecutado pruebas de recuperación, quedando pendiente de documentarlas.*
- *Se actualizara la información pertinente.*
- *Se creara la matriz de riesgos informáticos en el 2017.*



- Se detallan el estado de los documentos citados en "Normas Técnicas de Control Interno Específicas para el MINED, Definición de Políticas y Procedimientos de Controles Generales de los Sistemas de Información, Art. 323"...

| | |
|--|---|
| Portafolio de Proyectos y Servicios | Se procederá a actualizarlo |
| Catálogo de Servicio Basado en Tecnología de Información | Se procederá a actualizarlo |
| Manual de Procedimientos | Se procederá a actualizarlos |
| Plan de Infraestructura Tecnológica, del Ministerio de Educación | Se procederá a actualizarlo |
| Plan de Adquisiciones de Infraestructura Tecnológica | Se desarrollará |
| Plan de Contingencia de las Tecnologías de Información | Se procederá a actualizarlo |
| Plan de Mantenimiento de la Infraestructura Tecnológica | Se procederá a actualizarlo |
| Estándares de Seguridad de Tecnologías de Información | Ver respuesta en el primer literal de estos comentarios |

Comentarios de Auditoría Interna:

Al analizar los comentarios y pruebas de descargo presentadas por la Gerencia de Tecnología de Información y Comunicación (GTIC) se confirma nuestro hallazgo debido a lo siguiente:

- Los Estándares de Seguridad de Tecnologías de Información, no se encuentran elaborados, según lo manifestado por la GTIC donde toman el compromiso de consolidar las políticas de seguridad en un marco legal (confirmando la inexistencia del documento y que este se encuentra en elaboración).
- El documento de la Arquitectura de Información del MINED no fue proporcionado con la autorización correspondiente del CETI.
- Según los comentarios presentados por la GTIC el Plan de Contingencias de las Tecnologías de Información será actualizado y documentada las pruebas realizadas.
- Sobre la Matriz de Riesgos de Tecnología, la GTIC creara dicho documento en el transcurso del 2017.



HA-2: PROCESO TARDÍO DE CONTRATACIÓN DE LICENCIAMIENTO DE LOS SISTEMAS DE SEGURIDAD INFORMÁTICA.

| | |
|-----------------------------|------------------------|
| Importancia del Hallazgo: | Riesgo Alto |
| Componente NTCIE impactado: | Actividades de Control |

Observación:

Comprobamos que la Gerencia de Tecnologías de Información y Comunicación (GTIC), inicio tardíamente el proceso de contratación de los Sistemas de Seguridad Informática para el año 2016; debido a que, el requerimiento fue presentado a la Dirección de Contrataciones Institucionales el 22/07/2016 (ver **Gráfico No. 3**). Lo anterior, es agravante porque dicho licenciamiento se venció en junio de 2016 y a la fecha de este informe, se encuentra pendiente de emitir la orden de inicio, lo que, pone en riesgo la seguridad de la información.

Gráfico No. 3
Fluctuación del proceso de contratación para el año 2016



Al consultar con la GTIC, nos manifestaron que se debe a que el personal administrativo responsable del seguimiento a los planes de compra, fue trasladado a otra unidad del MINED y las actividades de esta naturaleza no fueron distribuidas y no existía personal responsable para ejecutar los procesos previos a la adquisición.

No obstante a lo anterior, existió seguimiento por parte de la Dirección de Contrataciones Institucional, sobre el proceso de licenciamiento, observando correos electrónicos de fecha 03/05/2016 y 14 y 21 de junio 2016; en donde, se les recordaba que no habían presentado los requerimientos para iniciar el proceso de compras, sin obtener respuesta sobre ello.



Normativa incumplida:

Normas Técnicas de Control Interno Especificas para el MINEDSeguridad de los Sistemas, Art. 339.- *“Las unidades de Informática, serán responsables de promover proyectos y procedimientos para proteger la información del MINED. Las Normas de Seguridad de la Información, estarán definidas en el Documento de Estándares de Seguridad de Tecnologías de Información”.*

Causa:

- Descuido de la Gerencia de Tecnologías de Información y Comunicación en realizar esa actividad antes que caducara la licencia de seguridad del año anterior.

Efectos:

- Vulnerabilidad a cualquier ataque informático a la Web, correos y sistemas del MINED.
- Exposición a los riesgos de TI y que las inversión en hardware o software de mayor envergadura, se direccionen erróneamente.
- Falta de Acciones que contrarresten la vulnerabilidad de los sistemas informáticos.

Comentarios de la Administración (Gerencia de Informática):

En atención al presente hallazgo de auditoría la Gerencia de Informática manifestó lo siguiente: *“Respecto al inicio tardío del proceso de contratación del licenciamiento de la plataforma de seguridad adjudicado a la GTIC, se tienen las pruebas de descargo siguiente:*

1. *Nota DFI-222 firmada por el Director Financiero Institucional, en donde notifica el 14 de abril de 2016, que hay que esperar la nueva normativa de austeridad de 2016 para poder hacer uso de recursos presupuestarios.*
2. *Correos de gestión de solicitud de fondos...”*

Comentarios de Auditoría Interna:

El comentario de la Gerencia de Informática expresa fundamentos sobre las acciones a seguir para evitar que esto vuelva a suceder; lo que, confirma nuestro hallazgo y plantea los hechos de comunicación que propiciaron el hallazgo de nuestra auditoría.



VII. RECOMENDACIONES

A la Dirección de Planificación:

1. Realizar las gestiones pertinentes para la autorización del Comité Estratégico de Tecnologías de Información (CETI) de los documentos a) Plan de Contingencias de las Tecnologías de Información y b) Metodología de Identificación de Riesgos Informáticos.
2. Presentar una propuesta de reubicación organizativa del Administrador de la Seguridad Institucional, al Comité Estratégico de Tecnologías de Información, a fin de mejorar las líneas de autoridad; consensuada con esta Dirección y la Dirección de Asesoría Jurídica.

A la Gerencia de Tecnologías de Información y Comunicaciones:

3. Iniciar los procesos de adquisición de las soluciones de seguridad y conexos, con anticipación a la finalización de las licencias en funcionamiento, con el objeto que el MINED no se encuentre descubierto antes las amenazas, ataques y vulnerabilidades de personal interno o externo y se cuenten con las estadísticas necesarias para el fortalecimiento del control.

VIII. SEGUIMIENTO DE AUDITORÍA

No se encontraron en nuestros registros, antecedentes de auditorías anteriores

IX. CONCLUSIÓN DE LA AUDITORIA

Conforme a los resultados obtenidos en la auditoria podemos concluir que el MINED ha estado expuesto a riesgo de ataques informáticos sin que se tomen las medidas oportunas para evitarlos, por no contar con el licenciamiento del sistema de seguridad antes que estas caducaran por descuido por parte de la GTIC; asimismo, existen vacíos legales al no contar con las normativas específicas autorizadas que administren, minimice y controlen los riesgos existentes; sin embargo, durante la auditoría la GTIC, tomó acción para contrarrestar dichos riesgos.



X. PÁRRAFO ACLARATORIO

El presente Informe se refiere únicamente a la auditoría por examen especial de tipo de gestión al Soporte de Licenciamiento del Software de Seguridad correspondiente al período de enero a diciembre del 2015 y de enero a octubre 2016 realizada en el MINED Central.

XI. AGRADECIMIENTOS

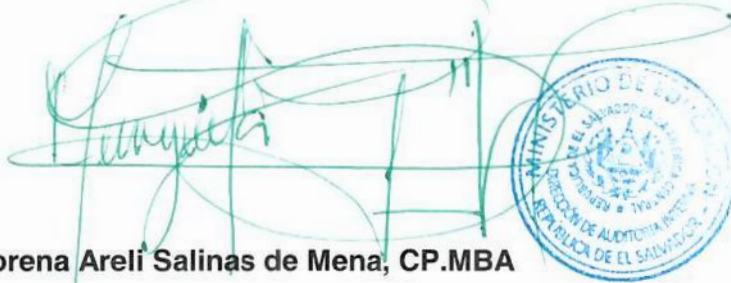
Hacemos extensivo nuestro agradecimiento al personal de la Dirección de Planificación, Dirección de Contrataciones Institucionales, Gerencia de Tecnologías de Información y Comunicación, por el apoyo brindado durante la ejecución de la presente auditoría.

XII. LUGAR Y FECHA

San Salvador, 29 de mayo de 2017.

XIII. FIRMA DEL RESPONSABLE DE LA DIRECCION DE AUDITORIA INTERNA

DIOS UNIÓN LIBERTAD



Morena Areli Salinas de Mena, CP.MBA
Directora
Dirección de Auditoría Interna, MINED
direcciondeauditoriainterna@mined.gob.sv

XIV. PERSONAL AUDITOR Y/O FUNCIONARIO QUE EJECUTÓ LA AUDITORÍA

██████████/Jefe de Auditoría

██████████/Jefe de Auditoría

Claudia Sánchez de Roque/Gerente de Auditoría Educativa y Administrativa