MINISTERIO DE ECONOMÍA

GOBIERNO DE EL SALVADOR

MINISTERIO DE ECONOMÍA

GERENCIA DE AUDITORÍA INTERNA

INFORME "AUDITORÍA ESPECIAL AL DESEMPEÑO Y SEGURIDAD DE LA RED INFORMATICA MINEC "

PERIODO 01 DE ENERO AL 30 DE JUNIO DE 2018

SAN SALVADOR, ENERO DE 2019

GOBIERNO DE EL SALVADOR
MINISTERIO DE ECONOMÍA

INDICE

INFORME DE AUDITORÍA
ESPECIAL AL DESEMPEÑO Y SEGURIDAD DE LA RED INFORMATICA MINEC
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
01 ENERO AL 30 DE JUNIO 2018

A. INTRODUCCIÓN

El presente informe, contiene el resultado del examen efectuado al Desempeño y Seguridad de la Red de Datos y Telecomunicaciones MINEC, Secretaría De Estado, la cual es administrada por la Gerencia de Seguridad y Telecomunicaciones de la Dirección de Tecnologías de la Información, durante el período del 01 de enero al 30 de junio de 2018.

El examen se realizó de conformidad con lo establecido en las Normas de Auditoría Interna del Sector Gubernamental, emitidas por la Corte de Cuentas de la República, en cumplimiento al Plan Anual de Trabajo que esta Gerencia desarrolla en el presente año.

B. ASPECTOS GENERALES

La Dirección de Tecnologías de la Información (DTI), tiene como objetivo modernizar la gestión del Ministerio de Economía a través de la automatización integral de los procesos de las distintas áreas organizativas que la conforman, brindando servicios de análisis y desarrollo de sistemas, soporte técnico, asesoría técnica y capacitación; con el propósito de ayudar y facilitar el logro de los objetivos institucionales. Está conformada por un Director, un Gerente de Informática, Gerente de Seguridad Informática y Telecomunicaciones (a partir de mayo de 2018 hasta la fecha no se cuenta con persona a cargo de la gerencia), Jefe de División de Soporte Técnico e Infraestructura, el cual depende jerárquicamente de la Gerencia de Seguridad Informática y Telecomunicaciones, Jefe de División de Sistemas de Información Geográfica, Jefe de División de Desarrollo de Sistemas, así como por el personal técnico y administrativo. La DTI depende jerárquicamente de la Viceministra de Comercio e Industria.

C. OBJETIVO DE LA AUDITORÍA

Objetivo General

Determinar la situación actual, fortalezas y debilidades, de la red de datos, saber en qué situación está la red para tomar decisiones sustentadas de reemplazo o mejora. Evaluar la seguridad de las redes institucionales, tanto en red local, metropolitana, inalámbricas, correo electrónico, defensa contra amenazas, defensa perimetral. Así como el cumplimiento de normativas y leyes aplicables.

Objetivos Específicos

- Verificar que se está protegiendo la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte.
- Verificar que se tengan controles para evitar el acceso físico no autorizado, los daños e interferencias a la información de la institución.
- Verificar el equilibrio entre controles de seguridad perimetrales (LAN/WAN) e internos, frente a controles de seguridad en aplicaciones (defensa en profundidad).
- Sustentar la confianza que merece en materia de seguridad; es decir, medir su capacidad para garantizar la autenticidad, confidencialidad, integridad, disponibilidad, y auditabilidad (trazabilidad), (ACIDA) de los servicios prestados y la información tratada, almacenada o transmitida.
- Establecer las áreas críticas y el alcance de la auditoría.
- Establecer las condiciones reportables resultantes del Examen.

D. ALCANCE Y PROCEDIMIENTOS

El examen comprendió la revisión de la documentación y controles utilizados por la Dirección de Tecnologías de la Información, los procedimientos que se desarrollaron durante la evaluación, correspondiente al periodo del 01 enero al 30 de junio 2018, los cuales se detallan a continuación:

- Se verificó el cumplimiento con Políticas Informáticas, Reglamento para utilización de las TIC`s en el Sector Gubernamental, Normas Técnicas de Control Interno Específicas del MINEC,vigentes.
- Evaluación de la parte física de la red, condiciones del cableado estructurado, mantenimiento de la sala de servidores, gabinetes de comunicación, etiquetado de los cables, orden, limpieza.

- Se revisó el mantenimiento de los equipos de comunicaciones, inventario actualizado de los equipos de red, garantías, licenciamiento de software utilizado en servidores.
- Se realizaron mediciones del consumo de ancho de banda, se utilizó herramienta de monitoreo.
- Se verificó la administración de los eventos, tráfico, seguridad, control de cambios, administración de fallas, monitoreo, documentación y configuración.

- El Centro de Seguridad para Internet (CIS)[1], contiene 20 controles sobre mejores prácticas sobre Ciberseguridad, de estos se evaluaron únicamente 12. (1-Inventario y control de activos hardware, 3- Administración continúa de vulnerabilidades, 4- Uso Controlado de Privilegios administrativos,7- Protección para email y web browser, 8- Malware Defenses, 9- Limitación y control de puertos de red, 11- Configuración Segura de los equipos de red, 12- Defensa de borde, 14- Control de acceso basado en la necesidad de conocer protección de datos,15- Control de Acceso inalambrico,17- Implementar un programa de concienciación y entrenamiento de seguridad y 20- Pruebas de penetración y ejercicios del equipo rojo).
- Se revisó el Plan Operativo para verificar la ejecución de metas.
- Se verificó la actualización y autorización de los instrumentos normativos internos con que cuenta la DTI.

El examen, se hizo con la documentación y comentarios que proporcionaron los auditados, pruebas realizadas y mediante inspección visual de equipos.

E. PRINCIPALES LOGROS

Logros: A pesar de no contar con un Gerente en Seguridad Informática y Telecomunicaciones, el Jefe de Sección de Soporte Técnico e Infraestructura ha sido aplicado en mantener monitoreo constante, en cuanto a los controles de seguridad relacionado a:

1-Inventario y control de activos hardware, 3- Administración continúa de vulnerabilidades, 4- Uso Controlado de Privilegios administrativos,7- Protección para email y web browser, 8- Malware Defenses, 9- Limitación y control de puertos de red, 11- Configuración Segura de los equipos de red, 12- Defensa de borde y 15- Control de Acceso inalámbrico.

[1] Center for Internet Security, https://www.cisecurity.org, El cual contiene las mejores prácticas en controles de ciberseguridad (incluidos 20 controles).

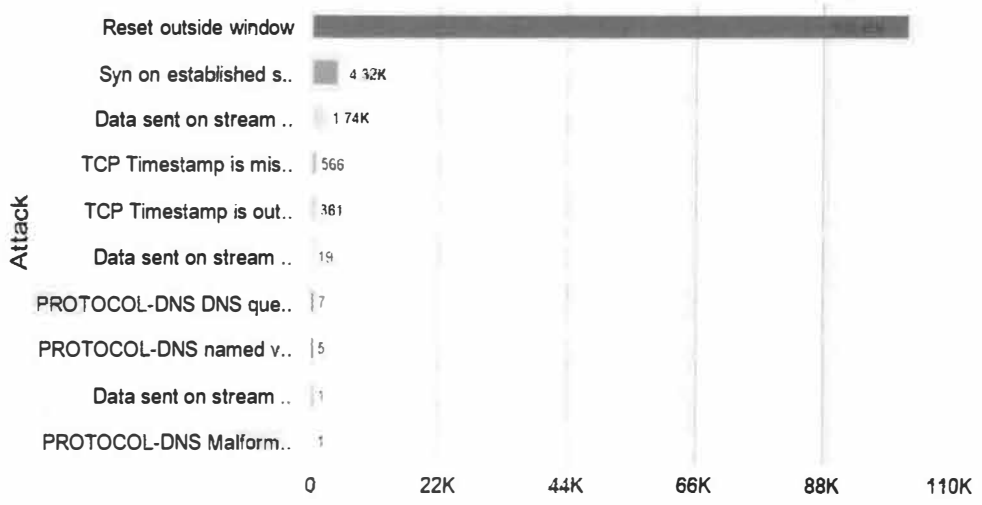
Se pudo comprobar que hasta la fecha del presente informe, no se han tenido ataques efectivos que hayan traspasado el "escudo protector", debido a que se han podido detectar a tiempo. Como muestra, se detalla a continuación un ejemplo de ataque.

Intrusion Attacks Report

2019-01-10 00:00:00 - 2019-01-10 23:59:59

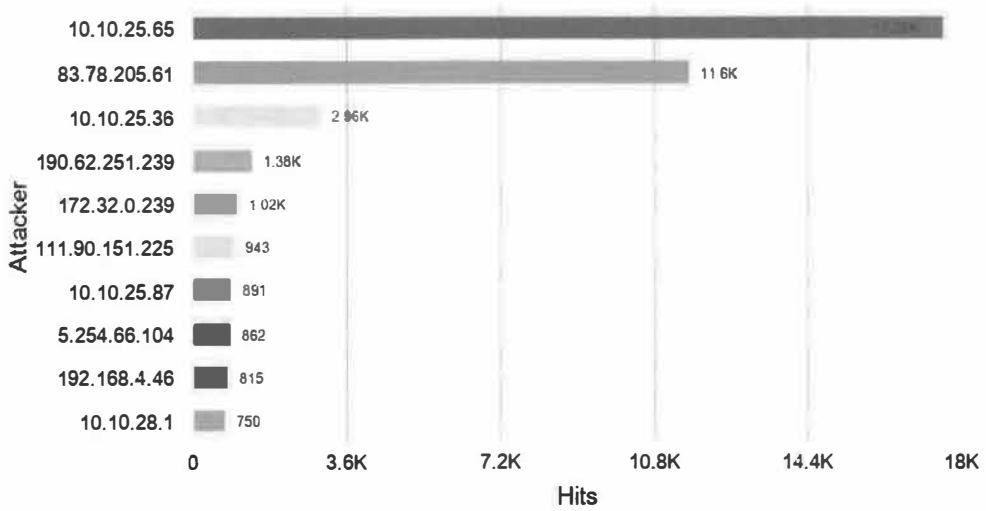
SOPHOS

Intrusion Attacks



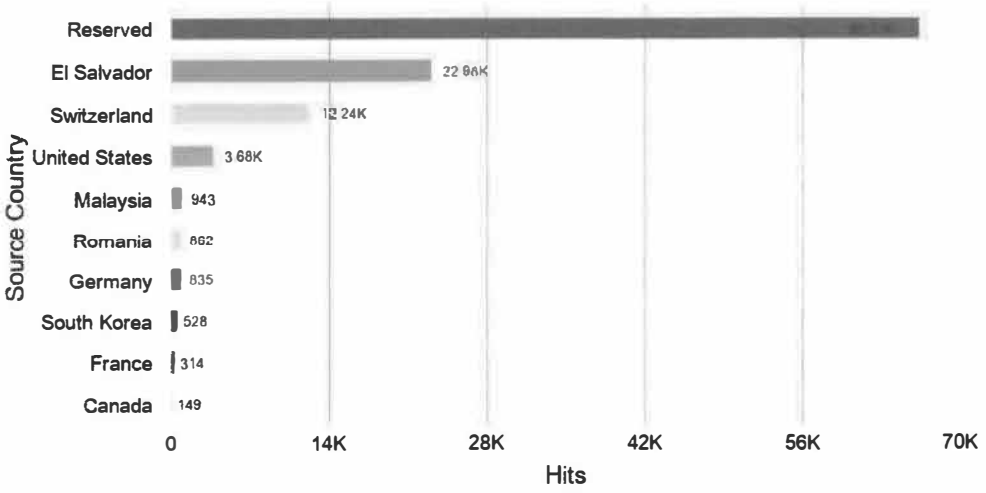
SOPHOS

Intrusion Source



SOPHOS

Source Countries



F. MARCO LEGAL

- Normas de Auditoría Interna del Sector Gubernamental,
- Normas Técnicas de Control Interno Específicas del MINEC,
- Ley de la Corte de Cuentas de la República,
- Reglamento para Uso y Control de las TIC en las entidades del Sector Público,
- Políticas Informáticas.

G. LIMITANTES DE LA AUDITORÍA

La evaluación se realizó específicamente a los aspectos indicados en el alcance y conforme los procedimientos de auditoría, por lo que pueden existir situaciones, que por encontrarse fuera del marco muestral y alcance delimitado, no hayan sido determinadas durante el examen.

No se realizaron pruebas de penetración de equipo rojo, solamente se evaluó el cuestionario de las preguntas del control y se solicitó evidencias. Esto debido a que no se cuenta con las herramientas y escenario para realizarlas.

Su realización implica posicionarse como un atacante potencial de manera remota y local, a través de técnicas de hackeo ético, se busca explotar activamente las vulnerabilidades de seguridad, tal como lo intentaría un intruso, se diseña y ejecuta escenarios reales que permitan identificar áreas de oportunidad para disminuir el impacto y la probabilidad de ciberataques. En la actualidad estas pruebas son muy costosas y requieren de un equipo de varios expertos en ciberseguridad y hackeo ético, así como de software y equipo especial.

H. RESUMEN DE RESULTADOS

Como resultado de los procedimientos de la auditoría realizado a la Seguridad de la Red del MINEC, no se determinaron condiciones relevantes; no obstante, se determinaron asuntos menores, relacionados con aspectos de control interno, los cuales son incorporados e informados en carta de gerencia.

I. SEGUIMIENTO DE AUDITORÍA

No se realizó seguimiento a las recomendaciones de las auditorías anteriores debido que los informes efectuados al área informática por Auditoría Interna, se les efectuó el respectivo seguimiento en su oportunidad, además, no se cuenta con informes de auditorías recientes al sistemas informático efectuados por la CCR.

J. CONCLUSIONES

Como resultado de la auditoría al Desempeño y Seguridad de la Red Informática del MINEC, concluimos:

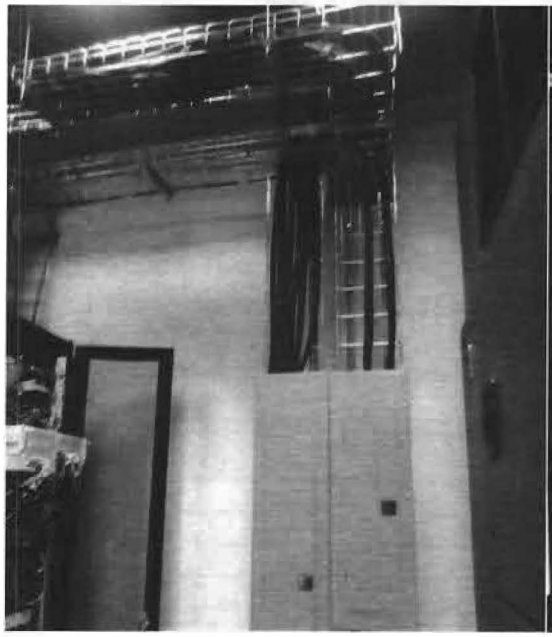
a) De los 12 controles que se evaluaron, 9 de ellos el porcentaje de aceptación ronda el 71.43% al 91.67%, sin embargo, en los controles 14 – Control de Acceso basado en la Necesidad de Conocer Protección de Datos, 17 – Control Implementar un programa de concienciación y entrenamiento de seguridad, 20 – Pruebas de penetración y ejercicios de equipo rojo, los porcentajes son muy bajos entre **0%** y **33.33%.** Como puede apreciarse en el siguiente cuadro.

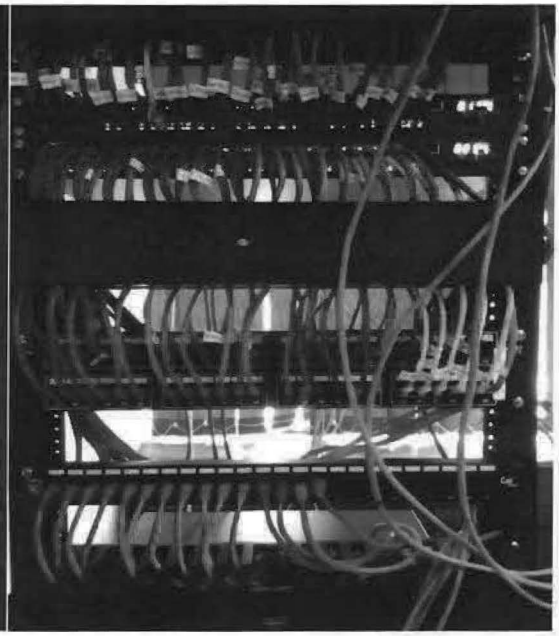
Evaluacion por cada Control CIS

Nº Control	CONTROLES CIS	Nº Preguntas	RESPUESTAS			Porcentaje		
			SI	NO	PARCIAL	SI	NO	PARCIAL
1	CIS - 1 Inventario y control de activos hardware	8	7		1	**87,5**	0	12,5
3	CIS -3 Administración Contínua de Vulnerabilidades	7	5	1	1	**71,43**	**20**	**14,29**
4	CIS - 4 Uso Controlado de Privilegios administrativos	9	8	1		**88,89**		
7	CIS - 7 Protección para Email y Web Browser	10	9		1	**90**		
8	CIS Control 8: Malware Defenses	8	6	2		**75**		
9	CIS Control 9: Limitación y control de puertos de red, protocolos y servicios	5	4	1		**80**		
11	CIS Control 11: Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores	7	5	1	1	**71,43**		
12	CIS Control 12: Defensa de borde	12	11		1	**91,67**		
14	CIS Control 14: Control de acceso basado en la necesidad de conocer Protección de datos	9	3	6		33,33		
15	CIS Control 15: Control de acceso inalámbrico	10	9	1		**90**		
20	CIS Control 20: Pruebas de penetración y ejercicios de equipo rojo	8		8		0		
17	CIS Control 17: Implementar un programa de concienciación y entrenamiento de seguridad	1		1		0		
		94	67	22	5			
Porcentaje Total de todos los controles			71,28	23,40	5,32			

En Anexo 1 Documentos probatorios se puede ver en detalle cada uno de las respuestas y sus documentos probatorios.

b) Se realizó un recorrido por los tres niveles de la Institución, y se procedió a verificar la parte física de la red, condiciones del cableado estructurado, observando que se encuentra en orden y etiquetado en "path panel" dentro de racks de piso, contando con su respectiva fuente de alimentación ininterrumpida, en lugar no accesible a usuarios, como se muestra en las tomas fotográficas siguientes:

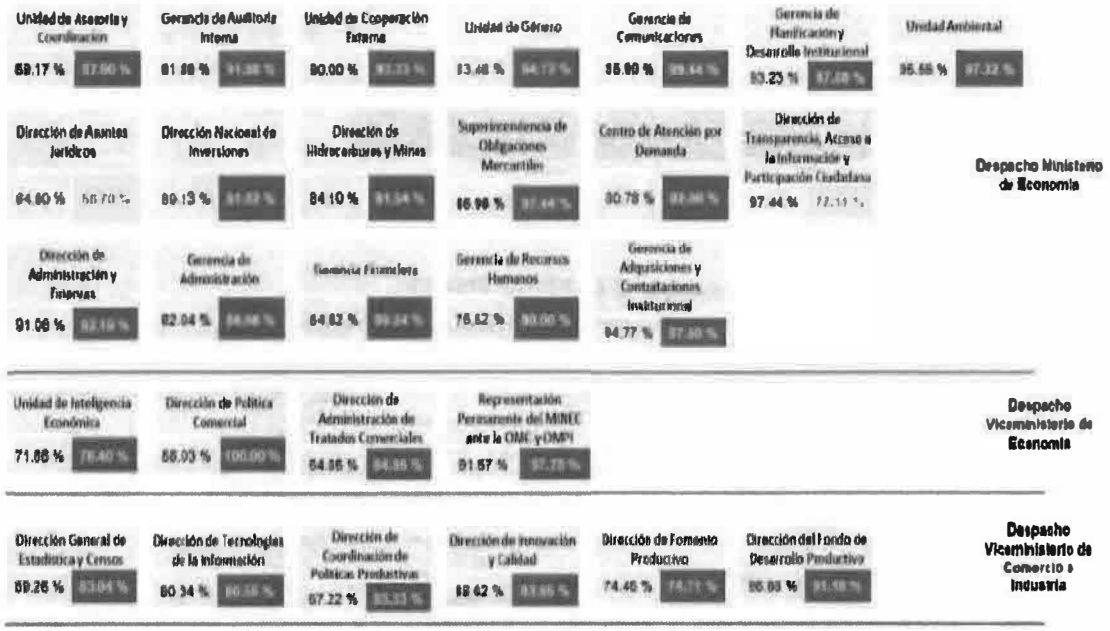




c) En el Manual de Organización y Funciones de la Dirección de Tecnologías de la Información, con fecha 18 de agosto de 2016, se pudo observar que en el Puesto Gerente de Seguridad Informática y Telecomunicaciones, su función básica es Administrar las telecomunicaciones, telefonía, red de datos y la seguridad informática institucional, haciendo uso eficiente de los recursos disponibles en la institución, que faciliten la ejecución de las funciones de los usuarios, dentro del marco legal vigente; a pesar de la importancia de su función básica, desde el mes de mayo de 2018, no se cuenta con personal a cargo de esta gerencia.

d) Plan Operativo Anual, para el mes de octubre de 2018, llevaba un 80% de ejecución de su plan operativo. Se detalla en el siguiente cuadro.

Plan Operativo Institucional 2018
Ejecución Acumulada de los Planes Anuales de Trabajo por Unidad Organizativa al mes de octubre



EL Trafico entrante (Traffic In) está representado de color verde claro, y el Trafico saliente (Traffic Out) de color rosado claro.

Se agradece a la Dirección de Tecnologías de la Información, específicamente al Jefe de Soporte Técnico e Infraestructura, por las facilidades y colaboración brindadas durante la ejecución de la auditoría; ya que contribuyó a la obtención de estos resultados.

K. PARRAFO ACLARATORIO

El informe se refiere a auditoría especial realizada a la Dirección de Tecnologías de la Información, específicamente a lo relacionado al Desempeño y Seguridad de las Redes Informáticas, tanto en datos como en telecomunicaciones, así como normativa interna, durante el período del 01 de enero al 30 de junio de 2018, por lo que no expresamos opinión sobre estados financieros o cifras contables, correspondientes a dicha área.

L. Anexo1 Documentos Probatorios.

DIOS, UNIÓN, LIBERTAD

Juan Alberto Castro
Auditor Interno, MINEC
San Salvador, 21 de enero de 2019