

Carta Circular N° 09 -GCTIC-ESSALUD-2019

Lima,

24 ENE. 2019

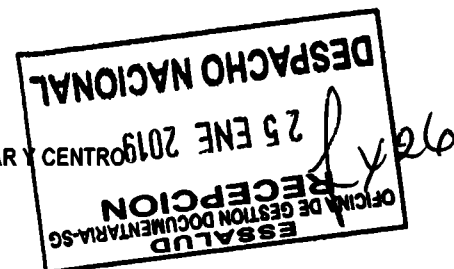
Señores

GERENTES DE REDES ASISTENCIALES A NIVEL NACIONAL

GERENTES DE REDES PRESTACIONALES: ALMENARA, REBAGLIATI, SABOGAL

GERENTE DE CENTROS ESPECIALIZADOS: INSTITUTO NACIONAL CARDIOVASCULAR Y NACIONAL DE SALUD RENAL

Presente. -

**Asunto** : Herramienta Oficial para la protección de dispositivos finales**Referencia** :
a) Carta Circular N° 072-GCTIC-ESSALUD-2012
b) Carta Circular N° 39-GCTIC-ESSALUD-2013
c) Carta Circular N° 44-GCTIC-ESSALUD-2013
d) Carta Circular N° 20-GCTIC-ESSALUD-2018

Es grato dirigirme a ustedes para saludarlos cordialmente y a la vez manifestarles que este despacho, dentro del ámbito de sus competencias, orientado a definir las políticas de seguridad informática e implementar las medidas de protección adecuadas para resguardar la integridad de la información, a pesar de las reiteradas comunicaciones señaladas en las referencias a), b), c) y d), viene observando que los clientes antivirus no se han instalado en la totalidad de equipos de cómputo desplegados a nivel nacional. (la relación de licencias instaladas se puede visualizar en anexos)

La herramienta oficial de ESSALUD para la protección Antivirus a nivel de dispositivo final es Sophos Endpoint Security and Control, la misma que además de los agentes instalados en los equipos, cuenta con una infraestructura de control centralizada, lo que nos permite intervenir de manera oportuna ante cualquier alerta o incidente, así mismo; existe infraestructura distribuida adicional destinada a la actualización de agentes y procedimientos asociados que permiten la gestión y operación de la plataforma.

En función a lo anteriormente señalado, como órgano encargado de establecer políticas que permitan una adecuada administración del hardware y software asignados a los órganos centrales y desconcentrados a fin de evaluar su cumplimiento; le solicitamos tenga a bien disponer, que bajo responsabilidad se dé cumplimiento a lo siguiente:

1. Todos los dispositivos finales que se conecten a la red institucional deben de contar con el agente de Sophos Endpoint Security and Control instalado.
2. Está prohibida la instalación de cualquier otra herramienta de seguridad a nivel de dispositivo final que no esté autorizada.

Cualquier consulta adicional, sírvase realizarla con el Ing. Larry Riega Riega, responsable de la gestión de la seguridad a nivel de dispositivos finales a través del anexo 2364 o de la cuenta de correo electrónico lriega@essalud.gob.pe

Sin otro particular y a la espera de la información solicitada, me despido de ustedes.

Atentamente,


Ing. JAVIER ALFARO PIZARRO
Gerente Central
Gerencia Central de Tecnologías de Información y Comunicaciones
ESSALUDJAP/ILLT/AHC/lrr
Nlt:100-2019-86
Folios: 09



"Año de la Lucha contra la corrupción y la Impunidad"

ANEXO A

Nº	DEPENDENCIA	PCS	Licencias Instaladas	DIFERENCIA
1	Lambayeque	1,621	780	841
2	La Libertad	1,786	1,022	764
3	Ica	1,268	621	647
4	Piura	1,045	476	569
5	Junín	1,066	570	496
6	Arequipa	1,445	961	484
7	Hospital Almenara	1,801	1,336	465
8	Cusco	837	520	317
9	Hospital Rebagliatti	1,722	1,451	271
10	Cajamarca	309	42	267
11	Huánuco	498	312	186
12	Puno	439	283	156
13	Apurímac	361	217	144
14	Cerro de Pasco	484	354	130
15	Ancash	571	453	118
16	Juliaca	377	270	107
17	Huancavelica	237	146	91
18	Amazonas	270	184	86
19	Ayacucho	359	284	75
20	Moquegua	401	330	71
21	Huaraz	202	133	69
22	Ucayali	266	208	58
23	Loreto	404	350	54
24	Tarapoto	335	285	50
25	Moyobamba	160	110	50
26	Madre de Dios	161	116	45
27	Incor	223	181	42
28	Tumbes	175	159	16
29	Centro Nacional de Salud Renal	144	134	10
30	Tacna	404	402	2
31	Hospital Sabogal	733	733	0



www.essalud.gob.pe

Jr. Domingo Cueto N° 120
Jesús María
Lima 11 – Perú
Tel.: 265-6000 / 265-7000



EsSalud

"Año de la Lucha contra la corrupción y la Impunidad"

ANEXO B

Nº	RED PRESTACIONAL ALMENARA	PCS	Licencias Instaladas	DIFERENCIA
1	Policlínico San Luis	65	38	27
2	Hospital II San Isidro El Labrador	91	64	27
3	Hospital III de Emergencias Grau	336	310	26
4	Hospital II Vitarte	153	127	26
5	Policlínico Chosica	73	49	24
6	Hospital I Jorge Voto Bernales Corpancho	113	95	18
7	Policlínico Francisco Pizarro	91	74	17
8	Centro Médico Ancije	56	41	15
9	CAP III Alfredo Piazza Roberts	60	45	15
10	CAP III El Agustino	70	58	12
11	CAP III Independencia	67	55	12
12	Sede Administrativa	86	74	12
13	Hospital I Aurelio Díaz Ufano y Peral	152	144	8
14	Hospital II Ramón Castilla	152	145	7
15	CAP III Huaycan	62	55	7
16	Posta Médica Construcción Civil	14	8	6
17	Centro Médico Casapalca	15	9	6

Nº	RED PRESTACIONAL HNERM	PCS	Licencias Instaladas	DIFERENCIA
1	Policlínico Próceres	69	49	20
2	CAP III Surquillo	38	29	9
3	Hospital II Suarez-Angamos	152	147	5
4	Hospital II Cañete	77	72	5
5	CAP III San Isidro	29	24	5
6	Centro Médico Mala	24	20	4
7	Policlínico Pablo Bermudez	111	108	3
8	Policlínico Santa Cruz	26	23	3
9	Policlínico Juan José Rodríguez Lazo	80	79	1
10	Policlínico Central de Prevención Larco	42	42	0
11	Sede Administrativa	98	98	0
12	CAP II Lurin	29	29	0
13	CAP III San Juan de Miraflores	70	70	0
14	Hospital I Uldarico Rocca Fernandez	110	110	0
15	Hospital I Carlos Alcántara Buterfield	114	114	0
16	Policlínico Chíncha	103	103	0



www.essalud.gob.pe

Jr. Domingo Cueto Nº 120
Jesús María
Lima 11 – Perú
Tel.: 265-6000 / 265-7000

+ 06

Nº	RED PRESTACIONAL SABOGAL	PCS	Licencias Instaladas	DIFERENCIA
1	Sede Administrativa	117	35	82
2	CAP III Pedro Reyes Barboza	43	25	18
3	CAP III Carabaylo	56	44	12
4	CAP III Puente Piedra	61	49	12
5	Hospital II Lima Norte "Luis Negreiros Vega"	190	179	11
6	Policlínico Fiori	77	66	11
7	Policlínico Complejidad Creciente El Retablo	51	41	10
8	CAP III Luis Negreiros	76	67	9
9	Hospital I Marino Molina Scippa	178	173	5
11	CAP II Chancay	35	31	4
12	PM Raura	5	1	4
13	Hospital II Gustavo Lanatta Luján	172	169	3
14	CAP III Hermana Maria Donrose Sutmolfer	79	76	3
15	CAP II Paramonga	28	25	3
16	PM Oyón	8	5	3
17	PM Humaya	5	4	1
18	CAP III Huaral	50	50	0
19	CAP II Sayán	16	16	0
1	Sede Central	2,952	2,687	265



CARTA CIRCULAR N° 072 OCTIC-ESSALUD-2012

Lima, 27 SET. 2012

Señores
JEFES DE OFICINA DE SOPORTE INFORMÁTICO DE REDES ASISTENCIALES
Presente.

Asunto : Acciones que se deben realizar en las computadoras personales

Es grato dirigirme a usted, a fin de solicitar la ejecución urgente de acciones correctivas, para mejorar el nivel de seguridad de las computadoras personales, las mismas que se detallan en los Anexo 1 y 2.

1. Actualizar la configuración del proxy en las computadoras de las redes asistenciales
2. Realizar la actualización de parches de las computadoras de las redes asistenciales
3. Si las mismas PC's después de las modificaciones indicadas en el punto 2, siguen siendo detectadas como infectadas en las herramientas de monitoreo que se tiene en la Sede Central, estas deberán ser formateadas según la red asistencial que corresponda.

Es preciso señalar, que las acciones serán realizadas por los Jefes de Soporte Informático respectivos.

Para tales acciones se ha elaborado un procedimiento que consiste en la actualización de los parches de seguridad de las computadoras, el mismo que se anexa al presente, que deberán ser ejecutadas sobre el resto de computadoras personales en un plazo no mayor de 3 meses.

Ante cualquier duda o consulta podrán comunicarse con los señores:

- Pumachagua Castillo Gomer gomer.pumachagua@essalud.gob.pe
- Larry Riega Iriega lriega@essalud.gob.pe
- Mesa de Ayuda, anexo 1111



Sin otro particular, quedo de usted,

Atentamente,

ELADIO VILLVERDE AGUILAR
Jefe de Oficina General
de Asesoría Jurídica y Asesoría Legal
ESSALUD

SMV/C28/MTV
MA 089-2012-470

EsSalud

"Decenio de la Persona con Discapacidad en el Perú"
"Año de la Inversión para el Desarrollo Rural y la Seguridad Alimentaria"

CARTA CIRCULAR N° 35 -OCTIC-ESSALUD-2013

Lima, 25 OCT. 2013

Señores

JEFES DE OFICINA DE SOPORTE INFORMÁTICO DE REDES ASISTENCIALES

JEFES DE INFORMÁTICA DEL CENTRO NACIONAL DE SALUD RENAL

JEFE DE INFORMÁTICA DEL INSTITUTO NACIONAL CARDIOVASCULAR (INCOR)

Presente.-

ASUNTO : ACTUALIZACIÓN DEL ANTIVIRUS CORPORATIVO EN LAS REDES ASISTENCIALES A NIVEL NACIONAL

REFERENCIA : Carta Circular N° 072-OCTIC-ESSALUD-2012

Es grato dirigirme a ustedes para informarles lo siguiente:

En los últimos días, se ha observado saturación de enlaces y caídas de conectividad a causa de ataques de códigos de malware desde la nube hacia EsSalud, que justamente tienen como destino, las direcciones IP de equipos informáticos que no tienen las actualizaciones de seguridad del fabricante Microsoft.

Es por ello se solicita a todos los Jefes de la Oficina de Soporte Informático de las Redes Asistenciales a nivel nacional, ejecuten en un corto plazo las tareas que adjunto remitimos:

- Instalación de los agentes del antivirus corporativo SOPHOS en todas las computadoras y servidores bajo su responsabilidad.
- Ejecutar los procedimientos de limpieza en aquellos que están notificados por nuestra consola Antimalware.
- Aplicar los parches y actualizaciones del sistema operativo Windows, donde aplique según procedimiento adjunto.

Debido a que no se ha visto avances significativos en el parchado de equipos enviado con Carta Circular N° 072-OCTIC-ESSALUD-2012, estamos procediendo a reiterar con el documento actual las recomendaciones puntuales del caso.

Agradeceré comunicarse con el Sr Larry Riega anexo 2364 o RPM #310595, personal de la Sub Gerencia de Soporte al Usuario de la Gerencia de Producción de esta Oficina Central, para que informen los avances de las acciones realizadas en cada uno de los Centros Asistenciales bajo su responsabilidad.

Sin otro particular, quedo de ustedes.

Atentamente,

Sr. GLADYS CRUZATI BARRERA
Jefe de Oficina Central
Oficina de Soporte al Usuario y Sistemas
ESSALUD

GCB/JS/PAWRT/ln
CC: GP, SGSU, OSI
N° 003-2013-470

Carta Circular N°

44

-OCTIC-ESSALUD-2013

Lima, 12 NOV. 2013

Señores
GERENCIA/DIRECCION DE ORGANO DESCONCENTRADO
GERENTE DE INSTITUTO/CENTRO ESPECIALIZADO
JEFES DE SOPORTE INFORMATICO
Presente.-

ASUNTO: Actualización de Antivirus Corporativo en las Redes Asistenciales a Nivel Nacional.

REFERENCIA : Carta Circular N° 072-OCTIC-ESSALUD-2012
Carta Circular N° 039-OCTIC-ESSALUD-2013

Es grato dirigirme a ustedes para informarles lo siguiente:

El software antimalware Sophos Endpoint Protection, desde Julio del presente año, es el único producto licenciado y autorizado por la institución para estaciones y servidores, que tiene como finalidad la protección permanente de los usuarios finales ante cualquier ataque de códigos de malware y pérdida de información dentro de la Red Corporativa.

Es responsabilidad del Jefe Informático de la Red Asistencial, que la actual solución se encuentre implementada en la totalidad de estaciones con sistema operativo Windows. Sin embargo, a pesar de las reiteradas comunicaciones a través de los documentos de la referencia, se puede evidenciar en el cuadro adjunto publicado que solo un departamento ha cumplido con las indicaciones establecidas, teniendo en cuenta que los procedimientos de instalación no requieren la implementación de ningún tipo de configuración previa, ya que los mecanismos de instalación como de actualización son totalmente transparentes para el usuario y son absolutamente sencillos, como se aprecia en la Intranet Institucional: <http://intranet.essalud/portal/sophos/>.

Es importante mencionar que, los equipos sin protección facilita el ataque de códigos de malware, provenientes de múltiples fuentes y ocasionan que saturan los enlaces de la red y dañen a las estructuras de directorios de windows, generando pérdida y daños a la información de nuestros usuarios.

Asimismo, se ha observado que la lentitud de enlaces y caídas de conectividad a causa de ataques de códigos de malware desde la nube hacia EsSalud, tienen como destino las direcciones Ip de los equipos que no tienen ni el cliente antivirus instalado, ni las actualizaciones de seguridad del fabricante Microsoft.

Al respecto, se encuentra alojado en la Intranet, las llaves de registro y el procedimiento respectivo para el parchado de equipos, que debe de ir en forma conjunta con la implementación de la solución antimalware, pudiendo ingresar a la dirección siguiente:

http://intranet.essalud/portal/zips/descargas/windows/Procedimiento_para_todas_las_computadoras_windows.pdf




Todas las estaciones que no reciben las actualizaciones de seguridad liberadas por el fabricante Microsoft y no tienen instalados el cliente antimalware corporativo, pueden ser infiltradas y controladas remotamente por el atacante.

Finalmente, se les solicita atender lo informado bajo responsabilidad en un **plazo no mayor de quince (15) días** a partir de la recepción de la presente, de lo contrario se procederá a informar a las instancias correspondientes.

Sin otro particular, quedo de ustedes.

Atentamente,




Sra. GLADYS CRUZATTI BAQUERIZO
Jefe de Oficina Central
Oficina Central de Tecnologías de Información y Comunicaciones
ESSALUD



GCB/JQS/WAT
CC GP, SGSU
NT 89-2013-440



"Año del Diálogo y la Reconciliación Nacional"
"Año del fortalecimiento de la atención primaria en EsSalud"

CARTA CIRCULAR N° 20 GCTIC-ESSALUD-2018

Lima, 15 JUN. 2018

Señores
GERENTES DE REDES ASISTENCIALES A NIVEL NACIONAL.
GERENTES DE REDES PRESTACIONALES: ALMENARA, REBAGLIATI Y SABOGAL.
GERENTES DE HOSPITALES NACIONALES: ALMENARA, REBAGLIATI Y SABOGAL
GERENTE DE CENTROS ESPECIALIZADOS: INSTITUTO NACIONAL CARDIOVASCULAR Y
CENTRO NACIONAL SALUD RENAL.
Presente.

Asunto: Herramienta Oficial para la protección de dispositivos finales.

Es grato dirigirme a ustedes para saludarlos cordialmente y comentarle que, a través de los procesos de revisión periódica, así como de las acciones de remediación de incidentes relacionados a la presencia de Malware, hemos detectado que se viene utilizando herramientas de protección distintas a la desplegada de manera oficial por ESSALUD.

Es por ello que vemos como necesario reiterar que la herramienta oficial de ESSALUD para la protección Anti Malware a nivel de dispositivo final es Sophos EndPoint Security and Control, la misma que además de los agentes instalados en los equipos cuenta con una infraestructura de control centralizada que nos permite intervenir de manera oportuna ante cualquier alerta o incidente, así mismo existe infraestructura distribuida adicional destinada a la actualización de agentes y procedimientos asociados que permiten la gestión y operación de la plataforma.


En ese sentido, como órgano encargado de establecer políticas que permitan una adecuada administración del hardware y software, asignados a los órganos centrales y desconcentrados, y evaluar su cumplimiento, le solicitamos tenga a bien disponer, que bajo responsabilidad se dé cumplimiento a lo siguiente:

1. Todos los dispositivos finales que se conecten a la red institucional deben contar con el agente de Sophos EndPoint Security and Control instalado.
2. Está prohibida la instalación de cualquier otra herramienta de seguridad a nivel de Dispositivo final que no sea Sophos EndPoint Security and Control.

Cualquier consulta o coordinación adicional sirvase realizarla con el Ing. Larry Riega Riega, responsable de la gestión de la seguridad a nivel de dispositivos finales a través del anexo 2364 o de la cuenta de correo electrónico lriega@essalud.gob.pe.

Sin otro particular y a la espera de la información solicitada, me despido de ustedes.

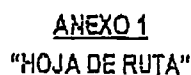
Atentamente,


Ing. Javier Alfaro Pizarro
Gerente Central
Gerencia Central de Tecnologías de Información y Comunicaciones
ESSALUD

JAP/CJO/UQF
c.c.: GPROD-SGST

NIT	100	2018	277
-----	-----	------	-----

Folios: 01)



NIT: 100-2019-86

Página. _____

IMPORTANTE: Mantener esta hoja de ruta como carátula del documento y utilizar el código de la acción solicitada

[illegible]

Cod. Acción sujeción

- 1 Atención
- 2 Opinión
- 3 Informe
- 4 Preparar respuesta
- 5 Coordinar

Cont. Agent solicited

6. Simular
7. Concientia y fines
8. Vigor
9. Archivo
10. Cms. - especificar

Pratt's House 10 272

Resolución de Gerencia General N° 1233-GG-ESSALUD-2017