



CHILQUINTA
servicios

GRUPO DE EMPRESAS CHILQUINTA

GERENCIA TECNOLOGIA

Identificación:
CS GT SGTI PO 12

Fecha Creación:
01-01-2015

Fecha Modificación:
10-12-2024

Versión:
0

PROCEDIMIENTO OPERATIVO

ADMINISTRACIÓN DE PARCHES DE SEGURIDAD

[SECURITY PATCH MANAGEMENT](#)

Revisado por:
Alfredo Martínez B.
Fecha: 10-12-2024

Aprobado por:
Wei Zhonghua
Fecha: 10-12-2024

1. OBJETIVO

El objetivo del siguiente documento consiste en definir las actividades y responsabilidades en el despliegue de parches de seguridad de los sistemas operativos, tanto para servidores como para las estaciones de trabajo de los usuarios, además de definir los canales de información que permitirán el conocimiento de la emisión de nuevos parches.

2. ALCANCE

Este procedimiento bajo alcance de Chilquinta Servicios S.A., aplicable bajo responsabilidad del área de Sistemas e Infraestructura, para todos los servidores y estaciones de trabajo de los usuarios pertenecientes al Grupo de Empresas Chilquinta.

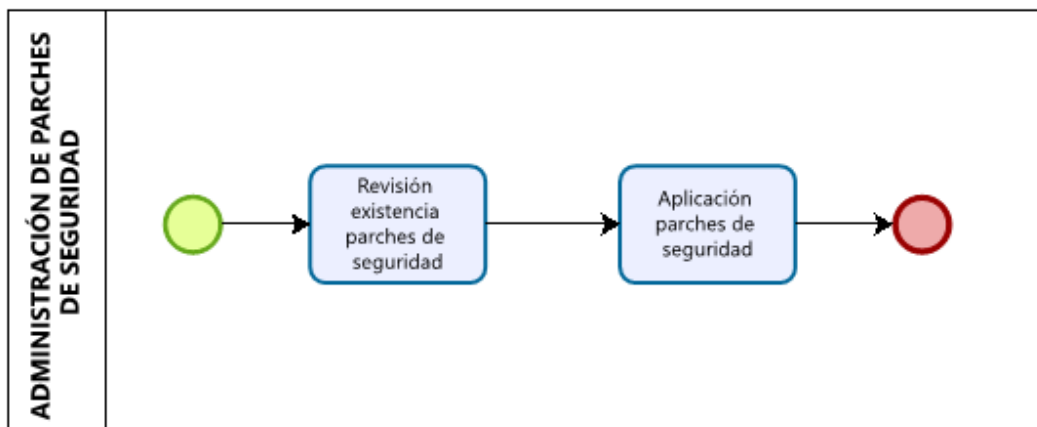
3. DEFINICIONES Y ABREVIACIONES

No Aplica.

4. RESPONSABILIDAD Y AUTORIDAD

CARGO	DESCRIPCIÓN
Ingeniero de Sistemas	Comprobar y verificar existencia de nuevos parches de seguridad.
Ingeniero de Ciberseguridad	Validar propuesta de parchado indicada por Ingeniero de Sistemas.
Administrador de Plataforma	Responsable de ejecutar el despliegue de parches de seguridad a través de las plataformas de parchado utilizadas, de acuerdo con lo indicado por Ingeniero de Sistemas o Ingeniero de Ciberseguridad.
Jefe de Sistemas e Infraestructura	Encargado de supervisar el despliegue de parches y mantener la planificación de estas actividades actualizadas.

5. DIAGRAMA DE FLUJO



6. CONTENIDO

- Se define como entrada del proceso de parchado las siguientes fuentes:

- ✓ Boletín Microsoft (<http://technet.microsoft.com/es-es/security/bulletin>)
- ✓ Software WSUS (Windows Server Update Services)
- ✓ Software Vicarius Topia (Plataforma Parchado).

- Se define como salida del proceso de parchado el registro de control de cambio.
- Se utilizan las herramientas WSUS y Vicarius Topia debido a que permiten la distribución de los parches y actualizaciones publicadas por Microsoft de forma centralizada.
- El Ingeniero de Sistemas debe validar la existencia de nuevos parches de seguridad y revisar si existe alguna actualización de carácter crítico, tanto para la plataforma de servidores, como para los endpoints, actividad validada por los Ingenieros de Ciberseguridad.
- En caso de recibir un informativo asociado a la existencia de un nuevo parche o actualización de seguridad, el Ingeniero de Sistemas deberá evaluar la factibilidad de implementación de este, analizando impactos y riesgos asociados para, finalmente, planificar el despliegue en conjunto con Ciberseguridad y los responsables del servicio involucrado.
- Los parches críticos de estaciones de trabajo para los usuarios se actualizan mediante las funcionalidades provistas por WSUS y/o Vicarius Topia.
- Los parches críticos a nivel de servidores, conectados al dominio, se actualizan mediante las funcionalidades provistas por WSUS y/o Vicarius Topia.
- Los parches críticos que, luego de la evaluación y compatibilidad con la plataforma de software instalada en servidores, corresponda aplicar serán gestionados mediante el correspondiente documento de Control de Cambio.
- Los parches críticos evaluados por el Ingeniero de Sistemas y que afecten a servidores de aplicaciones, deberán ser planificados en conjunto a Desarrollo de Proyectos y Sistemas de información, evaluando las ventanas de tiempo para su aplicación.
- La implementación de parches de seguridad se realiza de acuerdo con el Procedimiento Control de Cambios al Ambiente Operativo.
- Los parches críticos son aplicados en primera instancia en los servidores de los servicios, que cuentan con ambiente de desarrollo.
- Para los servidores de AD la instalación se realiza primero en alguno de los servidores, que no tenga roles.
- Con periodicidad trimestral se deberá revisar la existencia de actualizaciones para HP System Management Homepage.
- Los parches críticos de estaciones de trabajo para los usuarios se actualizarán mediante las funcionalidades provistas por WSUS y Vicarius Topia en forma automática, pidiendo reinicio del equipo a los usuarios.
- La periodicidad del despliegue de parches, para el caso de los endpoints, se realizará de forma mensual, principalmente a aquellos que sean críticos y que no posean errores (bug).

- La periodicidad del despliegue de parches, para el caso de la plataforma DMZ, se realizará de forma semestral.
- La periodicidad del despliegue de parches, para los demás servidores, se realizará de forma anual.
- Existen servidores excepcionados debido a restricciones de producto y restricciones de parches del creador como, por ejemplo, SCADA, PowerON y Open Smartflex.

7. NORMATIVA VIGENTE

No Aplica.

8. REFERENCIAS

Procedimiento Control de Cambios

9. ASUNTOS ÉTICOS

Consultas o inquietudes relacionadas con temas éticos pueden ser realizadas al encargado de cumplimiento (Gerente Legal) al fono: 322452289.


10. HISTORIAL DE CAMBIOS

Nº Versión	Fecha Vigencia	Comentario	Elaborado por	Revisado por	Aprobado por
0	01/01/2005	Creación y emisión de documento.	NA	NA	NA
1	06/01/2014	Revisión de documento.	NA	NA	NA
2	15/06/2015	Incorporación de WSUS.	NA	NA	NA
3	05/01/2017	Actualización de procedimiento.	NA	NA	NA
4	17/06/2017	Se adiciona la actualización de HP SMH.	NA	NA	NA
5	29/07/2017	Se realiza modificaciones de acuerdo con nueva estructura organizacional.	NA	NA	NA
6	09/09/2019	Se actualizan áreas y cargos por modificación de nombres de TYS a Infraestructura TI.	NA	NA	NA
7	29/05/2020	Revisión de documento.	NA	NA	NA
8	02/07/2020	Se eliminan puntos asociados a Sempa.	NA	NA	NA
9	17/07/2020	Modificación de formato.	NA	NA	NA
10	15/08/2021	Modificación de formato.	NA	NA	NA
11	31/01/2022	Revisión y actualización de cambios según GED.	NA	NA	NA

12	10/07/2023	Incorporación de plataforma Vicarius Topia.	NFG	NA	NA
0	10-12-2024	Actualización de formato, según Procedimiento Control y Gestión de Documentos Corporativos	Jesus Ayala	Alfredo Martínez	Wei Zhonghua

11. ANEXOS Y REGISTROS

Registros: Los registros digitales se almacenarán según se indique en la planilla de gestión de configuración del área de Sistemas e Infraestructura.

		CHILQUINTA GROUP OF COMPANIES TECHNOLOGY MANAGEMENT	
Identification: CS GT SGTI PO 12	Creation date: 01/01/2015	Modification date: 10-12-2024	Version: 0
OPERATING PROCEDURE SECURITY PATCH MANAGEMENT <u>ADMINISTRACIÓN DE PARCHES DE SEGURIDAD</u>			

Reviewed by: Alfredo Martínez B. Date: 10-12-2024	Approved by: Wei Zhonghua Date: 10-12-2024
---	--

1. OBJETIVE

The objective of the following document is to define the activities and responsibilities in the deployment of security patches of the operating systems, both for servers and for the workstations of the users, in addition to defining the information channels that will allow the knowledge of the issuance of new patches.

2. SCOPE

This procedure under the scope of Chilquinta Servicios S.A., applicable under the responsibility of the Systems and Infrastructure area, for all servers and workstations of users belonging to the Chilquinta Group of Companies.

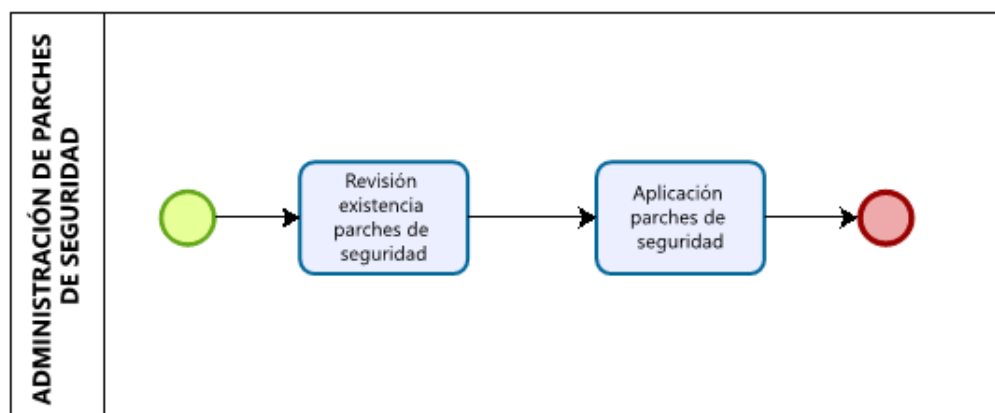
3. DEFINITIONS AND ABBREVIATIONS

Does not apply.

4. RESPONSIBILITY AND AUTHORITY

POSITION	DESCRIPTION
Systems Engineer	Check and verify the existence of new security patches.
Cybersecurity Engineer	Validate patching proposal indicated by Systems Engineer.
Platform Administrator	Responsible for executing the deployment of security patches through the patching platforms used, as indicated by Systems Engineer or Cybersecurity Engineer.
Head of Systems and Infrastructure	Responsible for overseeing the deployment of patches and keeping the planning of these activities up to date.

5. FLOWCHART



6. CONTENT

- The following sources are defined as the patching process input:

- ✓ Microsoft Newsletter (<http://technet.microsoft.com/es-es/security/bulletin>)
- ✓ WSUS Software (Windows Server Update Services)
- ✓ Vicarius Topia Software (Patched Platform).

- The change control record is defined as the output of the patching process.
- The WSUS and Vicarius Topia tools are used because they allow the distribution of patches and updates published by Microsoft in a centralized way.
- The System Engineer must validate the existence of new security patches and review if there is any update of a critical nature, both for the server platform, and for endpoints, activity validated by the Cybersecurity Engineers.
- In case of receiving an informative report associated with the existence of a new security patch or update, the Systems Engineer must evaluate the feasibility of implementing this, analyzing impacts and associated risks to, finally, plan the deployment in conjunction with Cybersecurity and the managers of the service involved.
- Critical workstation patches for users are updated using the functionalities provided by WSUS and/or Vicarius Topia.
- The critical patches at the server level, connected to the domain, are updated through the functionalities provided by WSUS and/or Vicarius Topia.
- The critical patches that, after evaluation and compatibility with the software platform installed on servers, apply will be managed through the corresponding Change Control document.
- The critical patches evaluated by the Systems Engineer and affecting application servers, must be planned in conjunction with Project Development and Information Systems, evaluating the time windows for their application.
- The implementation of security patches is done in accordance with the Procedure Control of Changes to the Operating Environment.
- The critical patches are applied in the first instance on the servers of the services, which have a development environment.
- For AD servers, the installation is done first on one of the servers, which has no roles.
- Updates for HP System Management Homepage should be reviewed on a quarterly basis.
- The critical workstation patches for users will be updated using the functionalities provided by WSUS and Vicarius Topia automatically, asking users to restart the computer.
- The periodicity of the deployment of patches, for the case of endpoints, will be done on a monthly basis, mainly to those that are critical and that do not have errors (bugs).
- The frequency of the deployment of patches, for the case of the DMZ platform, will be done on a biannual basis.

- Patch deployment periodicity, for all other servers, will be performed annually.
- Excepted servers exist due to product restrictions and creator patch restrictions such as SCADA, PowerON, and Open Smartflex.

7. REGULATIONS IN FORCE

Does not apply.

8. REFERENCES

Change Control Procedure.

9. ETHICAL ISSUES

Inquiries or concerns related to ethical issues can be made to the compliance officer (Legal Manager) at the phone number: 322452289.

10. CHANGE HISTORY

Version No	Effective Date	Comment	Prepared by	Reviewed by	Approved by
0	01-01-2005	Creation and issuance of documents.	NA	NA	NA
1	06/01/2014	Document review.	NA	NA	NA
2	6/15/2015	Incorporation of WSUS.	NA	NA	NA
3	05/01/2017	Procedure update.	NA	NA	NA
4	6/17/2017	HP SMH update is added.	NA	NA	NA
5	29/07/2017	Modifications are made according to new organizational structure.	NA	NA	NA
6	9/9/2019	Areas and charges for changing names from TYS to IT Infrastructure are updated.	NA	NA	NA
7	5/29/2020	Document review.	NA	NA	NA
8	02/07/2020	Points associated with Sempra are deleted.	NA	NA	NA
9	7/17/2020	Format modification.	NA	NA	NA
10	8/15/2021	Format modification.	NA	NA	NA
11	01/31/2022	Review and update of changes according to GED.	NA	NA	NA
12	7/10/2023	Incorporation of Vicarius Topia platform.	NFG	NA	NA
0	10-12-2024	Format update, according to Procedure Control and	Jesus Ayala	Alfredo Martínez	Wei Zhonghua

11. ANNEXES AND RECORDS

Records: The digital records will be stored as indicated in the configuration management form of the Systems and Infrastructure area.