CONTENIDO

Nombre: Ricardo de Jesús Delgado Montes. Cargo: Coordinador Grupo de Trabajo de Servicios Tecnológicos.	Revisado y Aprobado por: Nombre: Oscar Javier Asprilla Cruz Cargo: Jefe Oficina de Tecnología e Informática	Aprobación Metodológica por: Nombre: Giselle Johanna Castelblanco Muñoz Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad Fecha: 2018-11-14

1 OBJETIVO

Definir las actividades a realizar para la instalación de parches de seguridad en aplicativos y sistemas de información para los cuales la Oficina de Tecnología e Informática (OTI) es responsable o custodio. A través de la descripción de las etapas de validación e instalación de parches que permitan mantener seguros los aplicativos y sistemas operativos de la infraestructura tecnológica de la Superintendencia de Industria y Comercio.

2 DESTINATARIOS

Este procedimiento aplica a los servidores públicos y/o contratistas que laboran en el Grupo de Trabajo de Servicios Tecnológicos, o quien haga sus veces.

3 GLOSARIO

ACTIVO: Conforme con la norma ISO 27000, un activo de información es "cualquier cosa que tiene valor para la organización" y se categoriza en información digital, hardware, información física, servicio, recurso humano y software.

CUSTODIO: Es un funcionario, grupo de funcionarios o una Unidad Organizacional, designados por el responsable, los cuales se encargan de mantener las medidas de protección sobre los activos de información.

DISPOSITIVO O MEDIO DE ALMACENAMIENTO: Bajo este grupo se incluyen todos los elementos que se utilizan para almacenar información tales como discos flexibles, discos duros, unidades de estado sólido, cintas, discos ópticos.

HARDWARE: Parte tangible de un sistema informático, que puede corresponder a componentes de tipo: mecánico, electrónico, eléctrico, o electromecánico.

INFORMACIÓN DIGITAL: Cualquier tipo de información contenida en un medio digital, bien sea en forma de base de datos, en forma de archivos digitales o de intercambio.

RESPONSABLE: Es un funcionario perteneciente a la OTI que toma decisiones sobre el manejo, protección, disposición y demás atribuciones del activo.

4 REFERENCIAS

Jerarquía de la norma	Numero/Fecha	Título	Artículo	Aplicación Específica
NTC-ISO-IEC	27002:2013	Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para la Gestión de la Seguridad de la Información.	Aplicación total.	Aplicación total.

5 GENERALIDADES

Los parches de seguridad constituyen una opción para que los distribuidores de software liberen actualizaciones de seguridad para sus aplicativos; sin embargo, se deben seguir unos pasos para garantizar la correcta aplicación de los parches sin afectar los servicios o aplicativos que ya están ejecutándose y que hacen parte de un proceso definido dentro de la entidad.
Entre estos pasos se incluye el sometimiento del nuevo parche de seguridad a un conjunto de pruebas y validaciones de estabilidad que típicamente se llevarán a través de un ambiente de pruebas.

6 REPRESENTACIÓN ESQUEMÁTICA DEL PROCEDIMIENTO

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
1	**VALIDAR LA PERTIENENCIA Y APLICABILIDAD DEL PARCHE DE SEGURIDAD.**	Necesidad de instalación de un parche. Registro de cambio en la herramienta tecnológica.	Validar la pertinencia de la instalación de un parche de seguridad, a través de las siguientes actividades: - Recibir las actualizaciones o notificaciones de aplicación de parches de seguridad. - Revisar la aplicabilidad del parche de seguridad. - Revisar los servicios, componentes, o aplicativos afectados.	Coordinador del Grupo de Trabajo de Servicios Tecnológicos Comité asesor de cambios CAB.	Aprobación del cambio por parte del comité asesor de cambios Correo de notificación del Gestor de cambios respecto a la aprobación del cambio por parte del comité asesor de cambios, en relación con la instalación de parches solicitada.

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
2	**INSTALAR EL PARCHE DE SEGURIDAD.**	Aprobación del cambio por parte del comité asesor de cambios Correo de notificación del Gestor de cambios respecto a la aprobación del cambio por parte del comité asesor de cambios, en relación con la instalación de parches solicitada.	Realizar la instalación del parche de seguridad, mediante la siguiente actividad: Ejecutar el plan de rabajo aprobado por el comité asesor de cambios (CAB).	Coordinador del Grupo de Trabajo de Servicios Tecnológicos Coordinador del cambio. Especialistas mesa de servicio.	Notificación mediante correo electrónico de la ejecución del plan de trabajo.
3.	**VERIFICACIÓN DEL FUNCIONAMIENTO DE LOS SERVICIOS, COMPONENTES O APLICATIVOS AFECTADOS.**	Notificación mediante correo electrónico de la ejecución del plan de trabajo.	Realizar la verificación del correcto funcionamiento mediante al ejecución de la siguiente actividad: -Realizar las pruebas funcionales de los servicios, componentes o aplicativos afectados.	Áreas funcionales. Coordinador del cambio.	Notificación por medio de correo electrónico del correcto funcionamiento de los servicios, componentes o aplicativos afectados. Realizar el cierre del cambio en la herramienta Tecnológica.

7 DESCRIPCIÓN DE ACTIVIDADES Y RESPONSABILIDADES

7.1 ETAPA 1. VALIDAR LA PERTIENENCIA Y APLICABILIDAD DEL PARCHE DE SEGURIDAD.

7.1.1 Recibir las actualizaciones o notificaciones de aplicación de parches de seguridad.

El Coordinador del Grupo de Trabajo de Servicios Tecnológicos, o quien él delegue, será el encargado de revisar y recibir las actualizaciones de seguridad o notificaciones de aplicación de parches de seguridad. Existen diferentes mecanismos para obtener actualizaciones de seguridad relacionadas con aplicativos, siendo la más común la actualización automática que viene configurada por defecto en el aplicativo.

Mediante la actualización automática, el aplicativo se conecta directamente con los servidores de distribución de actualizaciones del fabricante de software, compara el estado de versiones, módulos y parches instalados con respecto a los disponibles desde el fabricante y genera un mensaje de notificación para el administrador del aplicativo indicando la existencia de actualizaciones.

Adicionalmente, el Coordinador del Grupo de Trabajo de Servicios Tecnológicos, o quien él delegue, puede inscribirse en boletines de seguridad o listas de correo del aplicativo, las cuales regularmente difunden información sobre la existencia de actualizaciones importantes de seguridad.

7.1.2 Revisar la aplicabilidad del parche de seguridad

El Coordinador del Grupo de Trabajo de Servicios Tecnológicos, o quien él delegue debe hacer una evaluación de la necesidad de aplicar un parche de seguridad en función de las características del parche y los módulos funcionales de los aplicativos instalados en el activo. Para esto se debe realizar una solicitud de cambio en la herramienta tecnológica para tal fin, que posteriormente surtirá un proceso de evaluación y aprobación por parte del comité asesor de cambios (CAB).

En algunas circunstancias, los parches de seguridad están relacionados con módulos que no están implementados en los aplicativos y, por lo tanto, no hay justificación para la instalación del parche. En el caso de sistemas operativos, es común disponer de parches de seguridad aplicables a interfaces de conexión que los equipos de cómputo no tienen (por ejemplo, interfaz de modem); por lo tanto, en este caso, tampoco es justificable la instalación de un parche.

Aunque la información provista por el fabricante del software en ocasiones no indique de afectación a servicios, componentes o aplicativos instalados en el sistema operativo, se debe realizar un procedimiento de evaluación de estabilidad y funcionamiento del parche de seguridad en un ambiente de pruebas. Igualmente, para las actividades definidas en el plan de trabajo para la coexistencia de servicios, componentes o aplicativos, se debe realizar un proceso de evaluación de aplicabilidad del parche de seguridad. Por lo tanto, el Coordinador del Grupo de Trabajo de Servicios Tecnológicos, o quien él delegue, son los encargados de solicitar la creación de un ambiente de pruebas (si este no existe) sobre el cual realizar la instalación del parche de seguridad y se verificara la coexistencia de servicios, componentes o aplicativos, para lo cual se genera una solicitud de cambio de acuerdo al GS02-P04 Procedimiento de Gestión del Cambio Tecnológico.

7.1.3 Revisar los servicios, componentes, o aplicativos afectados

El Coordinador del Grupo de Trabajo de Servicios Tecnológicos, o quien él delegue, debe revisar los parches de seguridad con detenimiento para garantizar que no impiden la ejecución de servicios, componentes o aplicativos que ya se encuentran instalados y son funcionales. Por lo tanto, debe validar las características del parche (disponibles a través de la información provista por el fabricante del software) y los efectos o consecuencias que éste genera en razón de utilización de puertos, habilitación/deshabilitación de servicios del sistema operativo y configuraciones de tráfico de entrada o de salida para esta revisión, podría apoyarse en el personal de la OTI que sea el custodio de los servicios, componentes o aplicativos afectados. En caso de que se determine que la aplicación del parche de seguridad afecta la ejecución de servicios, componentes o aplicativos ya instalados, se deben evaluar las razones y revisar la posibilidad de hacer ajustes que permitan la coexistencia del parche de seguridad y de los servicios, componentes o aplicativos instalados.

7.2 ETAPA 2. INSTALAR EL PARCHE DE SEGURIDAD

7.2.1 Ejecutar el plan de trabajo aprobado por el comité asesor de cambios (CAB).

El Coordinador del cambio, debe gestionar la ejecución de las actividades descritas en el plan de trabajo, que permitan la instalación del parche de seguridad por parte de los especialistas de la mesa de servicios. Dentro de las actividades típicas se encuentra la actualización conjunta de varios componentes del sistema operativo donde se encuentran desplegados los servicios y/o aplicativos, para garantizar una completa compatibilidad

7.3 ETAPA 3. VERIFICACIÓN DEL FUNCIONAMIENTO DE LOS SERVICIOS, COMPONENTES O APLICATIVOS AFECTADOS

7.3.1 Realizar las pruebas funcionales de los servicios, componentes o aplicativos afectados.

El Coordinador del cambio, o el área funcional realizara las pruebas de funcionalidad del servicio, componente o aplicativo, posterior a la instalación del parche de seguridad y remitirá la notificación correspondiente del resultado de las

pruebas, si las mismas son exitosas, se procederá con el cierre del cambio en la herramienta tecnológica.

8 DOCUMENTOS RELACIONADOS

SC05-I01 Sistema de Gestión de seguridad de la Información -Política del SGSI.
GS01-P08 Procedimiento de Gestión del Cambio Tecnológico.

9 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

1. Se realiza el cambio de código documental debido al cambio de proceso. Código anterior GS02-P06.
2. Se ajustan los códigos a la documentación relacionado en el procedimiento.
3. Se ajusta nombre del Grupo de Trabajo de Servicios Tecnológicos y Seguridad digital por Grupo de Trabajo de Servicios Tecnológicos.
4. Se actualizan las etapas y actividades del procedimiento.

Fin documento