CONTENIDO

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

1.OBJETIVO GENERAL

Entregar a los usuarios los servicios de TIC, conforme a los niveles de servicio acordados y con los controles de seguridad definidos.

1.1 OBJETIVO ESPECIFICOS

- Establecer mecanismos para administrar y operar la infraestructura y servicios de TIC, de manera que puedan resistir fallas, ataques deliberados o desastres y, se recuperen los servicios de TIC de manera ágil y segura.

- Asegurar la estabilidad y continuidad de la operación de la infraestructura de TIC en la aplicación de cambios y la solución de problemas e Incidentes, la implementación de aplicativos de cómputo, soluciones tecnológicas y nuevos servicios de TIC.

2.ALCANCE

El presente proceso de administración de operaciones y procesos TIC, nos ayudara a definir las tareas y los procesos que se deben ejecutar periódicamente y a conformar una programación formal de los procesos de la Oficina de Informática y Sistemas.

2.1. Roles del Proceso

- Responsable del Proceso de Administración de la Operación.
- Responsable del mantenimiento de la infraestructura.

3.REGLAS DEL PROCESO

- El responsable de este proceso estará a cargo de la operación y administración del centro de cómputo, o bien, del enlace con los responsables de los servicios que se encuentren contratados.

- El responsable de este proceso deberá revisar y en su caso, aprobar los cambios a los elementos o componentes del ambiente operativo.

- El responsable de este proceso, en coordinación con cada responsable de dominio tecnológico, se asegurará de que los servidores de cómputo de la red institucional, así como los componentes del ambiente operativo que manejen fecha y hora en sus sistemas operativos, se encuentren sincronizados a la hora oficial para Colombia.

- El responsable de este proceso se deberá asegurar que se realicen oportunamente las actividades, para determinar la efectividad de los controles de seguridad implementados.

- El responsable de este proceso deberá verificar que se siguen en todo momento los controles de seguridad establecidos en el SGSI.

4.ACTIVIDADES DEL PROCESO

4.1 AOP 1 Establecer el mecanismo de operación de los sistemas, aplicaciones y servicios de TIC.

4.1.1Descripción

Establecer las acciones a seguir para la programación, ejecución y seguimiento de las tareas de la operación de los sistemas, aplicaciones y servicios de TIC.

4.1.2 Factores Críticos

Desarrollar, implementar y mantener un mecanismo de operación de TIC para los sistemas, aplicaciones y servicios de TIC, que contemple las acciones a seguir para la programación, ejecución y seguimiento de las tareas de la operación, mantenimiento y respaldo; considerando al menos, lo siguiente:

- El cumplimiento de lo establecido en los programas de capacidad, de disponibilidad y de continuidad.
- Las tareas de entrega en turno (actividades, estado, actualizaciones finalizadas y en curso, problemas e incidentes de operación y de mesa de servicios, escalamientos y reportes sobre tareas relevantes pendientes de ejecutar o en seguimiento).
- Las actividades diarias que se deben ejecutar en cada activo de TIC, así como las que, en su caso, se deberán realizar de requerirse algún cambio en las actividades habituales.
- La elaboración de programas de ejecución de tareas para la operación de TIC, conforme a las necesidades de operación de la infraestructura y servicios de TIC.
- Los tiempos máximos permitidos para que un activo de TIC permanezca fuera de operación, por incidentes en la ejecución de tareas de la operación de TIC.
- Controles para el registro y seguimiento de incidentes en la ejecución de tareas de la operación de TIC.
- La identificación y aprobación de las salidas de las tareas de la operación de TIC.
- El manejo de excepciones, eventos e incidentes y cambios administrados, así como de controles de seguridad conforme al Proceso de Administración de la Seguridad de la Información y al Proceso de Operación de Controles de Seguridad de la Información.

Definir e implementar, en la medida de lo posible y conforme a las necesidades y recursos de la SuperVigilancia, herramientas tecnológicas para notificar y rectificar fallas críticas en las tareas de la operación, así como para monitorear el estado y operación de los dispositivos dentro de los límites aceptables, con la finalidad de prevenir fallas en la operación.

4.2 AOP 2 Programar y ejecutar las tareas de la operación de los sistemas, aplicaciones y servicios de TIC.

4.2.1 Descripción

Efectuar la programación de las tareas de la operación de los sistemas, aplicaciones y servicios de TIC, con base en el mecanismo de operación de TIC.

4.2.2 Factores Críticos

El responsable de este proceso deberá:

- Elaborar, conforme al mecanismo de operación de TIC, los programas de ejecución de tareas para la operación de TIC, que incluyan de manera

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

detallada y calendarizada: las tareas a desarrollar, por día y turno; el nombre de los responsables; los componentes y elementos de la configuración involucrados; el manejo de excepciones, eventos e incidentes y cambios.

- Coordinar la ejecución diaria de las tareas programadas para la operación de los sistemas, aplicaciones y servicios de TIC que se hubiere elaborado.

- Constatar que la persona a su cargo del proceso:

  - ✓ Ejecute las tareas contenidas en el programa de ejecución de tareas para la operación de TIC que les corresponda desarrollar y documentarlas en una bitácora de operación.

  - ✓ Registre y dé trámite a las solicitudes de cambio que deriven de la ejecución de las tareas de operación y efectuar tales cambios de manera administrada, estableciendo controles de seguridad en cada caso.

  - ✓ Registre y dé el trámite que corresponda a cualquier solicitud de servicio con motivo de incidentes de operación que deriven de la ejecución de las tareas de operación, y efectuar el seguimiento de la solicitud de manera administrada, estableciendo controles de seguridad en cada caso.

- Revisar las bitácoras de operación, para constatar que las tareas ejecutadas coinciden con las tareas programadas.

4.3 AOP 3 Monitorear la infraestructura de TIC en operación.

4.3.1 Descripción

Monitorear en los diferentes dispositivos de la infraestructura y de los servicios de TIC, la ejecución de las tareas de la operación, con el propósito de identificar eventos para prevenir o solucionar fallas e incidentes.

4.3.2 Factores Críticos

El responsable de este proceso deberá:

- Elaborar y mantener un listado de la información de la infraestructura y de los servicios de TIC cuya operación requiera monitorearse, con base en la información de los datos de los elementos de configuración correspondientes.

- Revisar que se registre cualquier tarea ejecutada como parte de la operación, a efecto de contar con registros que permitan identificar la causa raíz de incidentes, así como confirmar la ejecución satisfactoria de las tareas de la operación.

- Identificar los eventos que se presenten en la operación de la infraestructura y de los servicios de TIC, considerando al menos los eventos siguientes:

  - ✓ Alertas relacionadas con niveles máximos y mínimos de operación.

  - ✓ Alertas derivadas de alguna excepción en la secuencia de las tareas de operación.

  - ✓ Alertas por operación o comportamiento inusual.

Verificar que se hayan registrado en la bitácora de operación, los incidentes de la operación detectados, en el momento en que se presentaron.

Dar seguimiento a los eventos e incidentes que se presenten en la operación y registrar aquellos que aporten experiencia y conocimiento, con el propósito de apoyar el análisis para la solución de problemas o la prevención de incidentes, así como la mejora de las tareas de operación en la Entidad.

4.4 AOP 4 Implementar y verificar que se cumplan los controles de seguridad física en el centro de Computo.

4.4.1. Descripción

Implementar, de acuerdo con el SGSI, los controles de seguridad física en el centro de datos, así como para el acceso al propio centro y a los componentes o elementos del ambiente operativo, ubicados en el mismo.

4.4.2 Factores Críticos

El responsable del proceso, con apoyo de la persona encargada en la Seguridad de la Información, deberá:

- Definir un sistema de seguridad física en el centro de cómputo, en el que se incorporen, de acuerdo con el SGSI, los controles de seguridad para:

  - ✓ Los riesgos de seguridad física identificados en el Proceso de Administración de la Seguridad de la Información.
  - ✓ Limitar el acceso a la información sensible del centro de cómputo.
  - ✓ Efectuar el retiro, transporte y almacenamiento de activos de TIC, de forma segura.
  - ✓ El borrado seguro de la información de los dispositivos de almacenamiento fijos, removibles y externos, que sean retirados del ambiente operativo, por daño o reemplazo.
  - ✓ El registro de incidentes sobre la seguridad del ambiente físico, mediante la solicitud de servicio respectiva.

- Integrar al sistema de seguridad física en el centro de cómputo a que se refiere el factor crítico anterior, los controles de seguridad que de acuerdo con el SGSI se requieran para el acceso físico a las áreas reservadas de la Entidad, los cuales deberán considerar al menos los siguientes accesos:

  - ✓ Normal u ordinario.
  - ✓ Restringido.
  - ✓ Entrada o salida en caso de emergencia.
  - ✓ A equipos con datos sensibles.
  - ✓ A proveedores o visitantes.

- Integrar al sistema de seguridad física en el centro de datos, a que se refiere el factor crítico 1 anterior, los controles de seguridad que de acuerdo con el SGSI sean necesarios para hacer frente a los riesgos ambientales, considerando para ello:

  - ✓ Los riesgos por fenómenos naturales, identificados en el Proceso de Administración de la Seguridad de la Información.

- ✓ Los activos de TIC, incluyendo el equipo móvil y el que esté fuera del centro de datos.
- ✓ Los dispositivos que detectan amenazas ambientales, para responder a las alarmas y a otras notificaciones.

- Difundir al interior de la Entidad los controles de seguridad implementados y verificar su cumplimiento.

- Registrar los incidentes del ambiente físico que se presenten y administrarlos hasta su solución.

4.5 AOP 5 Elaborar y dar seguimiento al programa de aprovisionamiento de la infraestructura tecnológica.

4.5.1Descripción

Elaborar y dar seguimiento al programa de aprovisionamiento de la infraestructura tecnológica, para mantener la continuidad de la operación de los servicios de TIC.

4.5.2. Factores Críticos

El responsable del mantenimiento de la infraestructura, deberá:

Elaborar un programa de aprovisionamiento de la infraestructura tecnológica, el cual contendrá al menos:

- ✓ Los componentes que requiere y la justificación de los mismos, con base en el programa de tecnología y los servicios de TIC que soportará o complementará.

- ✓ La estimación de costos, beneficios, vida útil, disponibilidad de soporte técnico y/o mantenimiento, periodo de permanencia en el mercado, y apego a estándares tecnológicos.

- ✓ La fecha estimada en que se requerirá contar con cada componente.

El responsable del mantenimiento de la infraestructura deberá:

- ✓ Dar seguimiento al avance del programa de aprovisionamiento de la infraestructura tecnológica.

- ✓ Efectuar revisiones periódicas a la infraestructura tecnológica e identificar las posibles actualizaciones o mejoras a la misma, para efectos de que sean incluidas en el plan de adquisición de la Entidad para el aprovisionamiento de la infraestructura tecnológica.

4.6 AOP 6 Mantener los recursos de infraestructura tecnológica y su disponibilidad.

4.6.1 Descripción

Elaborar, ejecutar y dar seguimiento al programa de mantenimiento de la infraestructura tecnológica, e integrar controles de seguridad en la configuración, instalación y mantenimiento de componentes en la infraestructura

4.6.2 Factores Críticos

El responsable del mantenimiento de la infraestructura deberá:

- ✓ Elaborar un programa de mantenimiento de la infraestructura tecnológica que contenga acciones de carácter preventivo para evitar fallas a los componentes de dicha infraestructura, y difundirlo a los responsables de los procesos de la UTIC que estén involucrados.

- ✓ Aplicar los controles de mitigación de riesgos establecidos en el Proceso de Administración de la Seguridad de la Información, relativos a componentes de infraestructura.

- ✓ Asegurar que el programa de mantenimiento de la infraestructura tecnológica se ejecute por medio de cambios administrados.

- ✓ Implementar, en la realización de las tareas de instalación y mantenimiento de la infraestructura tecnológica, los controles de seguridad del SGSI, que consideren cuando menos:

  a. La protección de los componentes que serán instalados o que recibirán mantenimiento.
  b. Efectuar el respaldo y protección de los datos almacenados en la infraestructura tecnológica, así como del software que se encuentre instalado.
  c. Verificar que el ambiente de desarrollo y pruebas sea el adecuado para efectuar las tareas de instalación o de mantenimiento a la infraestructura tecnológica.
  d. Verificar que el ambiente de desarrollo y pruebas a que se refiere el inciso anterior esté separado del ambiente operativo.
  e. Comprobar la funcionalidad, seguridad, disponibilidad e integridad de los componentes instalados o en mantenimiento, con el propósito de que operen adecuadamente y se cumpla con los acuerdos de niveles de servicio establecidos.
  f. Modificar, en los componentes instalados, las contraseñas originales, configuraciones y parámetros que puedan afectar la seguridad y suprimir los accesos temporales utilizados en la instalación.
  g. Verificar que la instalación de software se efectúe de acuerdo con las especificaciones del mismo y que cualquier desviación sea identificada para evaluar su impacto, así como incluir la instalación de las actualizaciones de seguridad disponibles.
  h. Verificar que el software sea instalado con los privilegios mínimos necesarios a usuarios y administradores del software, así como que se hayan aplicado las recomendaciones de seguridad emitidas por el fabricante y por el SGSI para el fortalecimiento de la seguridad del software instalado.

- ✓ Evaluar la efectividad de los controles de seguridad aplicados en la instalación de los componentes y en las tareas de mantenimiento.

- ✓ Registrar y dar seguimiento a los incidentes de mantenimiento, con el propósito de analizar y eliminar las vulnerabilidades dentro de la infraestructura tecnológica.

- ✓ Diseñar el ambiente que permita la creación y simulación de pruebas de concepto y prototipos para verificar la viabilidad de componentes de infraestructura y de soluciones tecnológicas.

- ✓ Registrar el resultado de las pruebas realizadas y mantenerlas disponibles como información de conocimiento.

5. INDICADOR DEL PROCESO

INDICADOR	
Nombre	Incidentes en el ambiente operativo.
Objetivo	Medir la eficiencia en el proceso
Descripción	Obtener el número de Incidentes en la operación resueltos mediante la aplicación del mecanismo de operación de TIC.
Formula	% de eficiencia = (incidentes en la operación resueltos / incidentes que se presentaron en el ambiente operativo) X 100.
Responsable	El responsable de este proceso.
Frecuencia del calculo	Mensual

6. DEFINICIONES

AOP: Administración de Operaciones y Procesos

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co