Política de Respuesta Ante Incidentes

Introducción

Se define incidente a cualquier evento que desvíe la operación normal de un servicio y cause una interrupción o reducción de la calidad del mismo. La gestión de incidentes es un proceso continuo utilizado para administrar y minimizar el impacto de los eventos que comprometan la confidencialidad, integridad, disponibilidad de los servicios de Tecnología Informática (TI) del Gobierno de San Juan (GSJ).

Objetivo

Establecer lineamientos que permitan corregir con la máxima celeridad posible, las consecuencias y efectos negativos de los incidentes de los servicios de TI, a fin de minimizar su impacto.

Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GSJ.

Contenido

El objetivo de la gestión de incidentes es recuperar la operación de los servicios estándar tan rápido como sea posible. La Dirección de Ciberseguridad (DCS), requiere que todos los servicios de TI cuenten con un soporte ante incidencias, y que se establezcan medidas y mecanismos que permitan prevenir y detectar a tiempo, la posibilidad de ocurrencia de todos los incidentes que sea posible prever. Algunos de ellos pueden ser: alertas o eventos que afecten a la infraestructura de TI y operaciones de los sistemas informáticos del GSJ; anomalías o eventos que afecten la confidencialidad, integridad o disponibilidad de la información del GSJ; fallas o errores en las aplicaciones del GSJ que afecten su normal funcionamiento. El responsable de cada servicio de TI disponible en el GSJ deberá asegurar un soporte para los incidentes que puedan ocurrir y garantizar la resolución de los mismos en tiempo y forma, aún ante la necesidad de escalamiento en niveles de soporte, ya sea en el GSJ o por un tercero. Todos los incidentes se clasifican de acuerdo a su prioridad y complejidad de resolución.

Requerimientos del soporte ante incidentes

Para cada servicio de TI, la DCS requiere que los usuarios cuenten con un único punto de contacto disponible para notificar los posibles incidentes. Asimismo, el responsable de cada servicio de TI deberá establecer un procedimiento formal de comunicación, junto con un procedimiento de respuesta que determine la acción a emprender al recibir un informe sobre un incidente y, luego de su tratamiento, verifique la efectiva resolución del mismo.

Marco Normativo de TI

Todos los usuarios deberán notificar los posibles incidentes y no intentarán, bajo ninguna circunstancia, explotar o probar un posible punto débil o vulnerabilidad en el esquema de seguridad establecido para los sistemas y componentes de la red de comunicaciones del GSJ y/o alguno de los servicios de TI brindados. El soporte ante incidentes generalmente se divide en niveles para atender de una forma más eficaz y eficiente a los usuarios. El número de niveles en los que se organiza el soporte depende de las necesidades de cada servicio.

La estructura generalizada de servicio de soporte multinivel se conforma por:

Soporte de Nivel 1

Es el nivel de soporte inicial, responsable de las incidencias básicas del usuario. Generalmente actúa como punto de entrada de todas las incidencias. La tarea principal en este nivel, apoyándose en el

formulario F204, es reunir toda la información del usuario y determinar la incidencia mediante un análisis de los síntomas expresados y la determinación del problema. En el soporte de Nivel 1 habitualmente se tratan problemas simples de resolución sencilla. El personal a este nivel podría tener conocimiento básico y general de los servicios.

Soporte de Nivel 2

Es el nivel de soporte especializado, donde se resuelven incidencias en redes de comunicación, sistemas de información, sistemas operativos y bases de datos, entre otras. Las personas encargadas de realizar este soporte, apoyándose en el formulario F204, deberán ser los Senior responsables del activo TI y/o los referentes de la Red de Informáticos del Gobierno Provincial (RIGoP) y contar con conocimientos avanzados de los servicios a los que brinda soporte, además de los conocimientos de Nivel 1.

Habitualmente los sistemas de soporte ante incidencias se gestionan con un máximo de tres niveles, siendo el tercer nivel el de mayor capacidad para resolver problemas. Sin embargo, pueden incorporarse más niveles de acuerdo con la necesidad de soporte del servicio, así como también se puede contar con soporte por parte del proveedor de un producto o servicio dentro de la jerarquía de niveles de soporte ante incidencias.