Universidad de Puerto Rico en Bayamón
Oficina de Sistemas de Información

Política y Procedimiento para Documentar, Manejar y Resolver Incidentes Técnicos

14 de mayo de 2007

Revisado: septiembre 2012

Política y Procedimiento para Documentar, Manejar y Resolver Incidentes Técnicos

APROBADO POR:

Dr. Arturo Avilés González
Rector

31- Oct - 2012
Fecha

Srta. Bárbara Landrau Espinosa
Directora OSI

31- Oct - 2012
Fecha

Tabla de Contenido

INTRODUCCIÓN

Una respuesta inmediata a los incidentes que podrían poner en riesgo la seguridad, integridad, confidencialidad y disponibilidad de los activos, servicios, datos, programados, redes y demás recursos de tecnologías de información es indispensable para garantizar la operación continua de una organización. Sin una política y procedimiento para documentar, manejar y resolver incidentes los recursos de tecnologías de información podrían estar comprometidos, violando políticas, estatutos o la confianza otorgada por los miembros de la comunidad universitaria.

Un plan de respuesta a incidentes bien planificado generará los siguientes beneficios:

- Minimizará el daño que un incidente podría causar en un momento específico de confusión.
- Una política planificada por adelantado es superior a una conceptualizada en el momento de crisis.
- Los detalles que normalmente podrían pasarse por alto se pueden documentar en el plan.
- Permite adelantar la aportación de las demás dependencias de la institución en las acciones para resolver un incidente.
- Establece y comunica las posibles consecuencias que puede generar un incidente a la administración universitaria.

La ventaja más significativa de tener un plan de respuesta a incidentes integrado a las políticas, planes y procedimientos es la reducción significativa de riesgos.

PROPÓSITO

El propósito de este documento es identificar y planificar consistente y eficientemente las responsabilidades, decisiones, acciones y canales de comunicación involucrados para manejar y mitigar un incidente.

ALCANCE

Este documento de política y procedimiento para manejar incidentes aplica a los servicios y sistemas de las áreas funcionales de la Oficina de Sistemas de Información de la Universidad de Puerto Rico en Bayamón.

ENTIDADES A QUE APLICA ESTA POLÍTICA

Esta política y procedimiento le aplica a todas las áreas funcionales de la Oficina de Sistemas de Información de la Universidad de Puerto Rico en Bayamón. Las áreas funcionales son las siguientes:

- Telecomunicaciones
- Servidores
- Servicios al Usuario
- Análisis y Desarrollo de Sistemas
- Operaciones

Exclusiones de esta Política

Se excluirá de esta política y procedimiento todo incidente que resulte o que provenga de los siguientes:

- Información no electrónica
- Copiadoras y Fax (excepto asuntos relacionados con el proceso de imprimir)
- Llamadas telefónicas
- Seguridad física
- Plan de contingencia y recuperación de desastres

DEFINICIÓN DE UN INCIDENTE

Se define como incidente a cualquier evento inesperado que podría poner en riesgo una operación, sistema o servicio. Una violación a la política de seguridad de las computadoras, servidores o redes, o a la política de uso ético legal de las tecnologías de la UPR se considera también un incidente. Otros eventos adversos que están cubiertos por esta política y procedimiento pueden incluir:

- ataques para denegar servicios (*"denial of service"*)
- daños realizados a las partes de un sistema
- infección maliciosa a través de virus, *"spyware"* o *"malware"*
- *"scanning"* o pruebas no autorizadas de la red
- detección de intrusos
- ataques a uno o varios componentes de la red

Los incidentes pueden estar clasificados como crítico o no-crítico. Los incidentes críticos requieren una respuesta inmediata por parte de un equipo constituido para manejar esta clase de incidentes ya que representan situaciones de alto riesgo o de naturaleza sensitiva. Los incidentes clasificados como no-críticos representan poco o un nivel aceptable de riesgo por lo tanto puede atenderse por la persona designada a estos fines. Se considerará un incidente como crítico cuando el mismo esté tipificado con antelación o cuando un oficial universitario así lo indique.

DEFINICIÓN DE UNA RESPUESTA APROPIADA A UN INCIDENTE CRÍTICO

A través de las acciones que llevemos a cabo una vez se identifica un incidente, comienza un proceso de comunicación, manejo y mitigación del posible daño. Por tal razón, es importante identificar los elementos que se consideran una respuesta apropiada a un incidente, según aplique.

1. Determine si efectivamente hubo un incidente y su extensión.
2. Asuma el control del incidente e involucre al personal apropiado para manejar la situación.
3. Informe a la gerencia sobre el incidente y cómo usted procederá a resolverlo.
4. El incidente debe ser anotado en el Registro de Incidentes.
5. Recopile información, entreviste a testigos, recopile evidencia y documente.

6. Controle el daño que pudiese provocar el incidente a la mayor brevedad posible para evitar su desplazamiento, diseminación o caos.
7. Ejecute el plan de mitigación o procedimiento para resolver el incidente.
8. Proteja los derechos de empleados, estudiantes y visitantes establecidos por ley y por las políticas institucionales.
9. Documente todas las acciones y resultados en el programado.
10. Evalúe en conjunto con la gerencia si fueron efectiva las acciones llevadas a cabo.

Tipos de Incidentes

Cada incidente nos presenta una problemática diferente con formas determinadas para identificar y responder al mismo. A continuación ofrecemos una lista como ejemplo de los diversos tipos de incidentes:

- Cancelación de una corrida de programa
- Acceso no autorizado
- *"denial of service"*
- *"malicious code"* o *"virus"*
- uso inapropiado de los recursos de la red
- falla de la red de comunicaciones
- falla en el cuadro telefónico
- falla en los programas de aplicaciones o bases de datos
- múltiples tipos

SEVERIDAD DE UN INCIDENTE Y TIEMPO DE RESPUESTA

En adición a identificar el tipo de incidente, hay que determinar la severidad de un incidente para determinar la prioridad como el mismo deberá ser atendido. Primero, se considerará de severidad uno (1) cualquier incidente que afecte a uno o más sistemas críticos. Segundo, se considerará de severidad dos (2) cualquier incidente que afecte a un sistema utilizado por el usuario. Tercero, se considerará de severidad tres (3) cualquier incidente que afecte algún recurso o sistema de menor importancia en la operación continua de la UPRB. A continuación le ilustramos en la siguiente tabla:

Severidad	Categoría	Tiempo de Respuesta	Tipo de Acción
1	Crítico	Inmediata	Continúa hasta su resolución dentro del mismo día
2	Normal	Hasta dos días laborables	Resolución dentro del horario regular de servicio
3	No crítica	Hasta cuatro días laborables	Resolución dentro del horario regular de servicio

PROCEDIMIENTO DE ADMINISTRACIÓN Y UTILIZACIÓN DE LOS RECURSOS

I Se registra el incidente o situación. Si la notificación proviene de un usuario, se le pide que especifique lo más detallado posible el problema o situación para saber como manejar el mismo. Se determina bajo qué categoría, área o tipo de trabajo cae: (Ejemplo: Crítico, Normal, Apoyo Técnico, Operaciones, Programación, etc.)

a. Telecomunicaciones
b. Computadora
c. Programación Sistemas Administratrativos
d. Programados de Microsoft ("Campus Agreement", "Select", MSDNAA)
e. Operaciones y Producción
f. "Hardware"
g. Fotocopiadoras
h. Impresoras

II El(la) Supervisor(a) lo asigna al personal responsable del área que aplique, y le da seguimiento para que se cumpla en un tiempo razonable.

III Se evalúa el incidente y se toman las siguientes acciones:

a. Se hace diagnóstico.

b. Se corrige el incidente y se documenta.

c. Se hacen recomendaciones de ser necesario en cuanto a programados y equipo, según lo que aplique y que cumpla con los estándares mínimos (cambio de equipo, compra de programados y decomisar equipo).

d. Se coteja si aplica Garantía ó Contrato de Mantenimiento.

IV Se enviará evidencia al usuario de cómo se resolvió el incidente ó situación.

V Periódicamente se hará un análisis y se producirán estadísticas para saber qué incidentes son más recurrentes, qué equipos son los que generan más problemas, qué oficinas requieren mayor apoyo técnico, etc.