1. OBJETIVO

Tiene como objetivo resolver cualquier incidente que cause interrupción en el servicio de informática de la manera más rápida y efectiva posible, determinando la causa raíz para evitar su repetición.

2. ALCANCE

Este procedimiento aplica a todos los servicios informáticos suministrados por el área de Informatica a la Beneficencia del Valle del Cauca E.I.C.E.

3. DEFINICIONES Y GENERALIDADES DEL PROCEDIMIENTO

Incidente: Se define como incidente a cualquier evento inesperado que interrumpa o que pueda poner en riesgo una operación, sistema o servicio.

Tipos de Incidentes: El área de Informatica ha clasificado los incidentes en dos tipos:

A. Incidentes de Seguridad Informatica

- **Acceso no autorizado:** Esta categoría comprende todo tipo de ingreso y operación no autorizado a los sistemas, tanto exitosos como no exitosos. Son parte de esta categoría Accesos no autorizados exitosos, sin perjuicios visibles a componentes tecnológicos, Robo de información, Borrado de información, Alteración de la información, Intentos recurrentes y no recurrentes de acceso no autorizado, Abuso y/o Mal uso de los servicios informáticos internos o externos que requieren autenticación
- **Denegación del Servicio:** Esta categoría incluye los eventos que ocasionan pérdida de un servicio en particular. Los síntomas para detectar un incidente de esta categoría son: Tiempos de respuesta muy bajos sin razones aparentes, Servicio(s) interno(s) inaccesibles sin razones aparentes, Servicio(s) Externo(s) inaccesibles sin razones aparentes
- **Código malicioso:** Esta categoría comprende la introducción de códigos maliciosos en la infraestructura tecnológica de la Entidad, son parte de esta categoría: Virus informáticos, Troyanos y Gusanos informáticos
- **Mal uso de los recursos informáticos:** Esta categoría agrupa los eventos que atentan contra los recursos tecnológicos por el mal uso. Comprende: Mal uso y/o Abuso de servicios informáticos internos o externos, Violación de las normas de acceso a Internet,

Mal uso y/o Abuso del correo electrónico de la Entidad, Violación de las Políticas, Normas y Procedimientos de Seguridad Informática

- **Escaneos, pruebas o intentos de obtención de información de la red o de un servidor en particular**: Esta categoría agrupa los eventos que buscan obtener información de la infraestructura tecnológica de la Entidad. Comprende: Sniffers (software utilizado para capturar información que viaja por la red) y Detección de Vulnerabilidades

La administración y manejo de incidentes informáticos están a cargo del Jefe de Informática, que con base en el análisis de riesgo anual (Formato SE-FO–007 Matriz de riesgos) del área de Informatica se genera y ejecuta el plan de acción para la mitigación de mismos. Con el ánimo asegurar la efectividad de los controles, el área de Informatica busca en lo posible implementar soluciones tecnológicas que ayudan a automatizar el control de los riesgos.

B. Incidentes de la Operación o funcionales

- Falla de la red de comunicaciones
- Falla en los programas de aplicaciones, base de datos o software de oficina
- Falla en Hardware y equipos activos
- Interrupción de la prestación de un servicio
- Etc.

La administración de incidentes operacionales o funcionales está a cargo del Jefe de Informática. El manejo y resolución de incidentes están a cargo del Jefe de Informática con apoyo del auxiliar de informática.

3.1. Productos y Servicios de Informatica y Telecomunicaciones

- Servicio de correo electrónico
- Servicio de acceso a Internet
- Servicio de conexión remota VPN
- Servicio AZEN
- Servicio de administración, instalación y mantenimiento de equipos de cómputo e impresoras
- Servicio de red y comunicación de datos
- Servicio de videobeam
- Servicio de páginas WEB corporativas
- Servicio de almacenamiento, backup y recuperación de datos de aplicativos
- Servicio soporte proceso de Sorteo de lotería

3.2. Niveles de Soporte

Nivel de Soporte	Integrantes	Modo de Contacto
Nivel 1	Auxiliar de informática	Telefónico, verbal, escrito vía correo electrónico
Nivel 2	Jefe de Informática	Telefónico, verbal, escrito vía correo electrónico
Nivel 3	Proveedores de informática	Telefónico, escrito vía correo electrónico y son coordinados por el Jefe de informática

3.3. Tipos de Prioridad

PRIORIDAD	EVENTOS
CRITICA	Servicio fuera de línea que afecta la operación del negocio, de impacto y urgencia alto. Aplica para todo lo que afecte el día de ejecución del sorteo de la lotería del Valle.
ALTA	Servicio con desempeño bajo que afecta de manera parcial la operación del negocio. Por ejemplo: Caída del servidor controlador de dominio, caída del servidor de correo, caída páginas WEB
MEDIA	Servicio con bajo desempeño que no afecta directamente la operación del negocio Problema en hardware o software que afecta a un usuario sin interrumpir el normal funcionamiento del negocio Error en programa sin interrumpir la operación del negocio Por ejemplo: Daño en disco duro de usuario, mal funcionamiento de impresoras, error en el office, virus.
BAJA	No se está afectando el desempeño del servicio pero se desea mejorar. Problema que se debe corregir, pero no afecta el normal funcionamiento Por ejemplo: Daño del mouse, teclado, acceso a una página WEB restringida, daño en el teléfono.

3.4. Tiempos de Atención

Prioridad	Nivel 1 y 2 (Tiempo de resolución)	Nivel 3 (Tiempo de resolución)
Crítica	1 Hora	Según acuerdo de servicio con proveedores
Alta	4 Horas	
Media	27 Horas	
Baja	45 Horas	

4. DESCRIPCIÓN DE LAS ACTIVIDADES

4.1. GESTION DE INCIDENTES

El procedimiento para documentar, manejar y resolver los incidentes del área de Informatica con el objetivo de prevenir o corregir una falla de seguridad, o de la operación o funcionalidad en los servicios es el siguiente:

4.1.1. El usuario, registra el incidente a través de correo electrónico o de manera verbal al auxiliar de informática o al jefe de informática.

4.1.2. El Jefe de informática analiza el caso y determina:

- La prioridad del incidente: Se determina con base en la evaluación de las características: Urgencia, Tendencia e Impacto.
- Asigna al auxiliar de informática que se encargará de resolver el incidente.
- El tiempo de solución está relacionado con la prioridad que se le haya asignado al caso.

4.1.3. La persona encargada de resolver el incidente debe efectuar las siguientes actividades en caso de que aplique:

- Determinar si efectivamente hubo un incidente y cuál es su alcance.
- Asumir el control del incidente y si es necesario, involucrar al personal apropiado para manejar la situación.
- Cuando el incidente sea de seguridad informática y se haya clasificado con prioridad critica, se debe informar a la Jefatura de Informatica.
- Investigar, analizar y documentar el incidente en el formato de atención a usuarios (Formato AA-FO-001 Atención Usuarios).
- Si el tecnico encargado del incidente no puede resolver el caso, este debe ser escalado al siguiente nivel, cuando el caso se encuentra en poder de un tercero o compañía de soporte, la responsabilidad del caso siempre estará en poder de la persona interna que escalo el problema.
- Mantener informado a los usuarios sobre las acciones que se están tomando en la solución del caso.

4.1.4. En incidentes de Seguridad. Cuando se desconozca la(s) causa(s) que dieron origen al incidente o cuando se desconozca la solución definitiva al problema, se debe efectuar un análisis más exhaustivo del problema presentado.

4.1.5. Es recomendable mantener informado al usuario sobre el estatus del problema, con el objetivo de disminuir el ruido por suposiciones o malinterpretaciones.

4.2. GESTION DE PROBLEMAS

Las funciones principales de la **Gestión de Problemas** son:

- Investigar las causas a toda alteración, real o potencial, del servicio de Informatica.
- Determinar posibles soluciones a las mismas.

La **Gestión de Problemas** puede ser:

Reactiva: Analiza los incidentes ocurridos para descubrir su causa y propone soluciones a los mismos.

Proactiva: Monitoriza la calidad de la infraestructura de Informatica y analiza su configuración con el objetivo de prevenir incidentes antes de que estos ocurran.

El procedimiento para la Gestión de Problemas de Informatica y Telecomunicaciones es el siguiente:

4.2.1. La Gestión de Incidentes es la más estrecha colaboradora de la Gestión de Problemas pues estos están habitualmente originados por:

- Incidentes recurrentes de los que se desconocen sus causas
- Incidentes aislados con alto impacto en la calidad del servicio que no han podido ser asociados a algún error conocido.

4.2.2. La Gestión Proactiva, cuyo objetivo es el de prevenir incidentes o problemas antes que estos ocurran, en este paso se debe:

- Monitorear toda la infraestructura de Informatica
- Realizar análisis de tendencias
- Mantener informada a toda la Entidad de las acciones o mantenimientos programados

4.2.3. Registro y Clasificación de los Problemas

- Identificación del problema
- Clasificar el problema según el tipo, urgencia, impacto y prioridad
- Asignar recursos
- Registrar el problema en el sistema de anomalías con el objetivo de realizar un análisis más exhaustivo del problema y poder determinar la causa origen y poder establecer un plan de acción para corregir el problema de forma definitiva.

4.2.4. Análisis y Diagnostico

- Realizar el análisis para determinar las causas del problema y para convertir el problema en un error conocido.
- Proporcionar las soluciones temporales a la gestión de incidentes para minimizar el impacto del problema hasta que se implemente los cambios necesarios que lo resuelvan definitivamente.

4.2.5. Análisis y Evaluación de Soluciones

Para cada solución propuesta se debe evaluar:

- El posible impacto de cada una de las soluciones en la infraestructura de Informatica.
- Los costos asociados a cada implementación.
- Que consecuencias pueden generar sobre acuerdos de niveles de servicio.
- Selección de la mejor solución.

Todos los eventos deben quedar registrado en el formato GC-FO-003 Formato Acciones Correctivas

5. DOCUMENTOS Y REGISTROS DE REFERENCIA

GC-FO-003 Formato de Acciones Correctivas
SE-FO–015 Mapa de riesgos informática
AA-FO-001 Atención Usuarios