FCPC de Cesantía privada de servidores públicos de carrera del Gobierno Provincial de Imbabura "FCPC-GPI"

Ibarra – Ecuador

MANUAL DE TECNOLOGÍAS - INCIDENCIAS

FCPC-GPI

11 DE ABRIL 2025

1. Introducción

El propósito de este manual es establecer procedimientos claros para identificar, reportar y manejar incidentes con el fin de prevenir riesgos en el desarrollo normal de operaciones del fondo.

Objetivo

Identificar y manejar incidentes para prevenir riesgos.

2. Definición de Incidente

Un incidente se define como cualquier evento no deseado que pueda causar lesiones personales, daños a la propiedad, interrupción de operaciones o pérdida de datos.

Ejemplos de incidentes incluyen accidentes de trabajo, errores en el manejo de equipos, ciberataques, accidentes, errores humanos, fallas de equipos, desastres naturales.

3. Proceso de Reporte de Incidentes

3.1 Identificación de Incidentes: Los colaboradores del equipo deben estar atentos a cualquier situación que pueda representar un riesgo, como condiciones de trabajo inseguras, comportamientos peligrosos o problemas de equipo.

3.2 Indicadores para reconocer un incidente potencial.

Reconocer un incidente potencial puede ser fundamental para prevenir problemas mayores en diversas áreas del fondo, de acuerdo al siguiente esquema:

Cambios inusuales en el comportamiento del sistema: Esto puede incluir tiempos de respuesta más lentos, errores frecuentes, o actividades inesperadas en sistemas informáticos o de red.

Patrones de tráfico inusual: Observar un aumento repentino en el tráfico de red o patrones de acceso inusuales podría indicar actividades sospechosas.

Alertas de seguridad: Las alertas generadas por sistemas de monitoreo de seguridad, antivirus, firewalls u otras herramientas de seguridad pueden indicar posibles amenazas.

Actividades inusuales del usuario: Accesos al sistema SFOND o a los datos fuera del horario habitual de trabajo, intentos repetidos de acceder a recursos no autorizados, o cambios repentinos en los privilegios de acceso pueden indicar comportamientos anómalos.

Informes de colaboradores: Los colaboradores pueden detectar actividades sospechosas o anómalas en el entorno de trabajo que podrían señalar un incidente potencial.

Se deberá fomentar una cultura de reporte de incidentes en el fondo por medio verbal y escrito.

Anomalías físicas: Anomalías como olores extraños, ruidos inusuales, o cambios en la temperatura de las máquinas o servidores pueden indicar potenciales riesgos.

Vulnerabilidades conocidas: La identificación de vulnerabilidades conocidas en sistemas, aplicaciones o infraestructuras puede indicar áreas propensas a ataques o fallos de seguridad.

Actividades sospechosas en medios digitales: En el ámbito de la reputación y relaciones públicas, la detección de comentarios negativos, rumores o actividades sospechosas en redes sociales o medios digitales puede indicar potenciales incidentes de relaciones públicas o crisis.

3.3 Responsabilidades de los colaboradores o miembros del equipo en la identificación de incidentes.

La identificación de incidentes es una responsabilidad compartida entre todos los miembros del equipo de trabajo, las cuales, se deberá identificar de forma inmediata:

Conocimiento de los procedimientos de seguridad: Todos los colaboradores deben estar familiarizados con los procedimientos de seguridad del fondo y saber cómo identificar posibles incidentes.

Vigilancia activa: Los colaboradores deben estar atentos a cualquier actividad inusual o sospechosa en sus áreas de trabajo, incluidos sistemas informáticos, redes, instalaciones físicas y otros activos del fondo.

Reporte de incidentes: Si un colaborador observa algo que podría ser un incidente de seguridad o una situación de riesgo, debe informarlo de inmediato a los canales apropiados designados por el fondo. Esto puede incluir el envío por medio físico a través de un oficio o por correo electrónico.

Participación en la formación y concienciación: Los colaboradores deben participar activamente en programas de formación y concienciación sobre seguridad, que les proporcionen los conocimientos necesarios para identificar y responder adecuadamente a los incidentes de seguridad, que sean propuestos por el ente administrador y/o de control.

Cumplimiento de las políticas de seguridad: Los colaboradores deben cumplir con todas las políticas y procedimientos de seguridad establecidos por el fondo, incluidas las políticas de acceso a sistemas, contraseñas, y protección de datos.

Mantenimiento de la vigilancia: Los colaboradores deben mantener una vigilancia continua y estar alerta a posibles amenazas de seguridad en todo momento.

Participación en ejercicios de simulación: Participar en ejercicios de simulación de incidentes puede ayudar a los colaboradores a familiarizarse con los procedimientos de respuesta y a mejorar su capacidad para identificar incidentes en situaciones reales.

Mejora continua: Los colaboradores deben estar dispuestos a aprender de los incidentes pasados y buscar formas de mejorar los procesos de identificación y respuesta a incidentes en el futuro.

3.4 Notificación del Incidente: Se debe reportar mediante comunicación interna al jefe inmediato superior, e informar sobre cualquier incidente tan pronto como sea posible.

La información requerida debe incluir fecha, hora, ubicación, descripción del incidente y personas involucradas.

3.4.1 Canal de comunicación designado para informar sobre incidentes. Un canal de comunicación designado para informar sobre incidentes debe ser accesible, confidencial, claro y eficiente, y debe estar respaldado por un proceso sólido de seguimiento y respuesta.

Esto ayuda a garantizar que los colaboradores puedan reportar incidentes de seguridad de manera rápida y efectiva, lo que a su vez contribuye a la protección del fondo contra posibles amenazas y riesgos.

Las características principales de los canales de comunicación son:
Accesibilidad: El canal de comunicación debe ser fácilmente accesible. Puede ser un oficio con firma de responsabilidad, una dirección de correo electrónico específica, o directamente al celular del jefe inmediato.

Disponibilidad: El canal de comunicación debe estar disponible las 24 horas del día, los 7 días de la semana, para que los colaboradores puedan informar sobre incidentes en cualquier momento, incluso fuera del horario laboral normal.

Confidencialidad: Se debe garantizar la confidencialidad de la información proporcionada a través del canal de comunicación designado.

Los colaboradores deben sentirse seguros al informar sobre incidentes sin temor a represalias o violaciones de privacidad.

Proceso claro de reporte: El proceso de reporte debe ser claro y bien definido para que los colaboradores puedan reportar incidentes de manera efectiva.

Esto puede incluir instrucciones detalladas sobre qué información proporcionar, cómo categorizar el incidente y a quién dirigirse en caso de preguntas o preocupaciones.

Seguimiento y respuesta oportuna: Una vez que se informa sobre un incidente, debe haber un proceso establecido para su seguimiento y resolución oportuna.

Los colaboradores deben recibir confirmación de que su informe ha sido recibido y actualizaciones periódicas sobre el progreso de la investigación y la resolución del incidente, el cual lo deben emitir el administrador del fondo.

Capacitación y concienciación: Es importante capacitar a los colaboradores sobre cómo utilizar el canal de comunicación designado y concienciarlos sobre la importancia de informar sobre incidentes de seguridad.

Esto puede incluir sesiones de formación periódicas, materiales de referencia y recordatorios regulares sobre la disponibilidad del canal de comunicación.

Integración con equipos de respuesta a incidentes: El canal de comunicación designado debe estar integrado con los equipos de respuesta a incidentes de la organización para garantizar una gestión eficaz de los incidentes reportados.

3.4.2 Procedimientos claros para reportar incidentes de manera rápida y efectiva.

Para reportar incidentes de manera rápida y efectiva, es crucial contar con procedimientos claros y bien definidos.

Educación y Concientización: Antes de que ocurran los incidentes, es fundamental educar a todos los colaboradores sobre qué constituye un incidente, por qué es importante reportarlo y cómo hacerlo correctamente.

Se deberán realizar sesiones de formación periódicas con los involucrados.

Canal de Reporte: Establece un canal de reporte centralizado y accesible para todos los colaboradores.

Puede ser un correo electrónico específico, un formulario de reporte o un oficio con firma de responsabilidad.

Formato de Reporte: Es un formulario o plantilla estándar para que los colaboradores reporten incidentes.

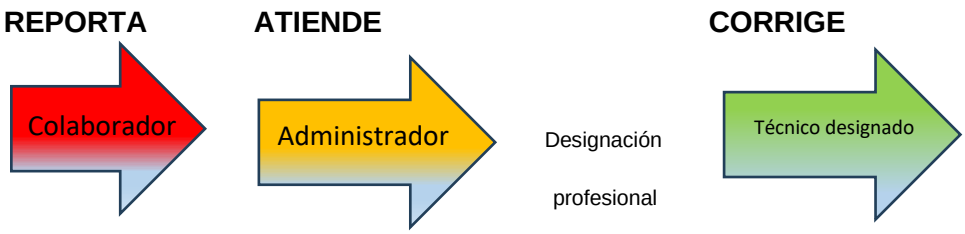
Este documento debe incluir campos como fecha, hora, descripción del incidente, impacto, personas afectadas, acciones tomadas y cualquier otra información relevante.

Priorización: Definir criterios claros para priorizar los incidentes según su gravedad, impacto y urgencia.

Esto ayudará a asignar recursos de manera eficiente y responder adecuadamente a cada situación.

Responsabilidades: Especifica quién es responsable de recibir, evaluar y gestionar los reportes de incidentes.

Deben designarse roles claros para garantizar una respuesta rápida y efectiva.



Escalación: Establece un proceso de escalación para incidentes graves o que requieran intervención de niveles superiores de la organización.

Define quiénes son las personas o equipos responsables de tomar decisiones en cada nivel de escalación.

Comunicación: Establece protocolos de comunicación claros para informar a todas las partes interesadas sobre el estado de los incidentes y las acciones tomadas.

Esto puede incluir actualizaciones periódicas por correo electrónico, reuniones de seguimiento o comunicados según la gravedad y la naturaleza del incidente.

Análisis Post-Incidente: Después de resolver un incidente, realiza un análisis detallado para identificar las causas subyacentes, las lecciones aprendidas y las medidas preventivas que se pueden implementar para evitar incidentes similares en el futuro.

Mejora Continua: Utilizar la retroalimentación recibida de los reportes de incidentes y del análisis post-incidente para mejorar continuamente los procesos y procedimientos de gestión de incidentes.

Pruebas y Simulacros: Realizar pruebas y simulacros periódicos para asegurar que todos los colaboradores estén familiarizados con los procedimientos de reporte de incidentes y sepan cómo actuar en caso de una emergencia real.

3.4.3 Información necesaria para incluir en el reporte de incidentes

Fecha y hora del incidente: Registra la fecha y la hora exactas en que ocurrió el incidente.

Esto ayuda a establecer un marco temporal para la respuesta y el seguimiento.

Descripción del incidente: Proporciona una descripción detallada del incidente, incluyendo lo que sucedió, cómo ocurrió y dónde ocurrió.

Cuanta más información se incluya, mejor será la comprensión del incidente.

Impacto: Evaluar el impacto del incidente en el fondo, los sistemas, los datos y las operaciones.

Describir cómo afectó a la operatividad normal del fondo y a los usuarios.

Personas involucradas: Identificar a las personas o equipos involucrados en el incidente, incluyendo aquellos que lo reportaron, los afectados directos e indirectos, y cualquier persona que haya participado en la respuesta inicial**.**

Recursos afectados: Hacer una lista los sistemas, aplicaciones, datos u otros recursos que se vieron comprometidos o afectados por el incidente.

Esto puede incluir servidores, redes, bases de datos, archivos o dispositivos.

Evidencia o registros: Adjuntar cualquier evidencia relevante, como registros de eventos, capturas de pantalla, correos electrónicos sospechosos, archivos maliciosos o cualquier otro artefacto digital relacionado con el incidente.

Causa raíz: Intentar identificar la causa raíz o las causas subyacentes que contribuyeron al incidente.

Esto ayudará a implementar medidas preventivas para evitar incidentes similares en el futuro.

Acciones tomadas: Describir las acciones tomadas para responder al incidente, incluyendo quién las llevó a cabo, cuándo se realizaron y qué resultados se obtuvieron.

Esto puede incluir medidas de contención, recuperación de datos, parcheo de sistemas, entre otras.

Comentarios y observaciones: Proporcionar cualquier comentario adicional u observación relevante sobre el incidente, incluyendo lecciones aprendidas, recomendaciones para mejorar la respuesta en el futuro y cualquier otro detalle importante.

Firma y fecha: Firmar y fechar el reporte para confirmar su veracidad y proporcionar un registro oficial de cuándo se realizó.

3.5 Evaluación del Incidente:

El equipo técnico designado evaluará la gravedad del incidente y determinará la respuesta apropiada.

Se considerarán factores como la seguridad de las personas e información de los partícipes, el impacto en las operaciones y la posible causa del incidente.

3.5.1 Criterios para determinar la prioridad de respuesta.

Determinar la prioridad de respuesta en incidentes es crucial para asignar recursos de manera efectiva y minimizar el impacto en el fondo, se deben considerar los siguientes criterios:

Gravedad del incidente: Evalúa la gravedad del incidente en función de su impacto potencial en el fondo.

Por ejemplo, un incidente que cause interrupción del servicio para partícipes puede considerarse de mayor gravedad que un incidente que afecte solo a un área interna de la empresa.

Impacto operativo: Considera el impacto del incidente en las operaciones normales.

Si el incidente afecta críticamente la capacidad de operatividad del fondo para realizar sus funciones básicas, se considerará de alta prioridad.

Confidencialidad, integridad y disponibilidad de datos: Evalúa si el incidente compromete la confidencialidad, integridad o disponibilidad de datos sensibles o críticos para el fondo.

La pérdida o el acceso no autorizado a datos confidenciales puede justificar una respuesta prioritaria.

Potencial de propagación o escalada: Considera si el incidente tiene el potencial de propagarse a otros sistemas o áreas del fondo, o si podría escalar a un incidente más grande.

La detección temprana y la contención de incidentes con potencial de propagación pueden evitar daños adicionales.

Reputación y riesgo legal: Evalúa el impacto del incidente en la reputación del fondo y los posibles riesgos legales.

Incidentes que pueden afectar negativamente la imagen pública del fondo o resultar en responsabilidad legal pueden requerir una respuesta inmediata.

Exposición a terceros: Considera si el incidente afecta a partícipes, proveedores, u otras partes externas.

La exposición de terceros puede aumentar la prioridad del incidente debido a las implicaciones adicionales para la relación con las partes relacionadas.

Requerimientos reglamentarios: Evalúa si el incidente afecta el cumplimiento de regulaciones normativas del fondo, ya que al incumplir con los requisitos reglamentarios puede tener consecuencias legales y financieras significativas.

Capacidad de recuperación: Evalúa la capacidad de la organización para recuperarse del incidente. Si el incidente compromete sistemas críticos o infraestructura clave, puede ser necesario priorizar la respuesta para minimizar el tiempo de inactividad y los impactos financieros.

4. **Respuesta ante Incidentes externos que afecten la integridad del personal del fondo**

Acciones Inmediatas: En caso de un accidente grave, se activará el protocolo de emergencia y se llamará al personal de emergencias del 911.

Se evacuará el área si es necesario y se tomarán medidas para contener cualquier daño adicional.

Investigación del Incidente: El personal del fondo recopilará evidencia, entrevistará a testigos y analizará las causas del incidente para prevenir su recurrencia.

Comunicación y Notificación: Se informará al personal del fondo, y al ente administrador sobre el incidente y las medidas tomadas para abordarlo.

Si es necesario, se notificará al ente de control.

5. **Seguimiento y Acciones Correctivas**

Documentación y Registro: Se mantendrá un registro detallado de todos los incidentes reportados, incluidas las acciones tomadas y las decisiones clave.

Implementación de Medidas Correctivas: Se desarrollarán planes de acción para abordar las causas subyacentes del incidente, asignando responsabilidades y plazos para su implementación.

Monitoreo y Evaluación: Se realizará un seguimiento regular del progreso de las medidas correctivas y se revisarán periódicamente para garantizar su efectividad.

Capacitación y Sensibilización: Se llevarán a cabo sesiones de capacitación periódicas para todos los colaboradores sobre la identificación de riesgos, el reporte de incidentes y las medidas de seguridad.

Además, se promoverá una cultura de seguridad a través de campañas de sensibilización y comunicación interna.

Conclusiones

Este manual establece un marco sólido para la gestión de incidentes con el objetivo de prevenir riesgos y garantizar un entorno de trabajo seguro.

El compromiso de todos los miembros del equipo es fundamental para su éxito continuo.

DISPOSICION FINAL

El presente documento entrará en vigencia a partir de la fecha de la Resolución de aprobación por parte del Representante Legal del **FCPC DE CESANTIA PRIVADA DE SERVIDORES PUBLICOS DE CARRERA DEL GPI.**

Ibarra, 11 de abril 2025.

Mgs. María Isabel Realpe G.

ADMINISTRADORA FCPC GPI