**UNIVERSIDAD CATÓLICA LUIS AMIGÓ**

**Procedimiento para reportar un incidente de**

**seguridad de información personal**

Un incidente es todo suceso que compromete o es capaz de comprometer alguno de los aspectos relacionados con la seguridad de la información personal, fundamentalmente confidencialidad, integridad y disponibilidad, cualquiera que sea el soporte (usb, portátil, disco duro ó extraíble, etc.) y el tratamiento que se haga sobre la misma. Independiente de la categoría de dato (público, semi-público, privado, sensible).

Cualquier persona de la Universidad Católica Luis Amigó que intervenga en el tratamiento de datos de carácter personal, así como en el desarrollo de actividades relacionadas con la seguridad de las mismas, puede detectar una incidencia.

Con el fin de optimizar la gestión de las incidencias que puedan producirse en la institución cada empleado de la universidad debe seguir esta ruta para reportar los incidentes de seguridad de la información personal de que tenga conocimiento, así sea por hurto, acceso no autorizado, etc,

* Reportar el hecho a infraestructura al correo: jefe.itecnologica@amigo.edu.co
* Quien analizado el caso y hecho la contención inicial adecuada e inmediata.
* Reportará a la coordinación de datos personales al correo: protecciondedatos@amigo.edu.co
* La persona implicada debe diligenciar el formato de reporte de incidente de seguridad de dato personal que será el insumo para el reporte ante la SIC.
* Como aspecto final el área de TI adoptará las medidas necesarias para que en la institución en el futuro no se vuelva a repetir el incidente.

Para la correcta gestión de los incidentes, y la minimización de los impactos ocasionados, debe existir un procedimiento conocido por todo el personal que trate datos de carácter personal, y que permita la comunicación, registro, seguimiento, respuesta y cierre de los mismos.

Las fases que debe cubrir dicho procedimiento son las siguientes:

1. La persona que detecta la incidencia, informa de la misma al departamento correspondiente, por cualquier medio a su alcance (*e-mail*, teléfono, intranet, etc.) o empleando cualquier otro recurso o herramienta de la organización.
2. Recibida la comunicación, el departamento correspondiente recaba todos los datos necesarios para abrir la incidencia (usuario que notificó la incidencia, fecha y hora en que se detectó, descripción de la incidencia) y la deriva al técnico correspondiente para su solución.
3. Una vez solucionada la incidencia, deberá registrarse especificando, al menos, la siguiente información: Tipo de incidencia, el momento en que se ha producido y/o detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.
4. La persona responsable de aplicar las acciones definidas, verifica la realización de las mismas y la resolución de la incidencia.

Cuando se deban aplicar medidas de nivel medio o alto y la acción de respuesta definida incluya la recuperación de datos, además de lo indicado en el procedimiento anterior, se registrará el responsable de la recuperación, los datos restaurados, en su caso, los datos que han sido necesarios grabar manualmente en dicho proceso de recuperación, así como la autorización por parte del responsable sobre el que se haya delegado la capacidad de autorizar la restauración de copias de seguridad.

Coordinación de Habeas Data