**Apéndice 1 – Plan de respuesta a los incidentes**

\*\* VERSIÓN DE MUESTRA GRATIS \*\*

**Historial de modificaciones**

|  |  |  |  |
| --- | --- | --- | --- |
| **Fecha** | **Versión** | **Creado por** | **Descripción de la modificación** |
| DD-MM-AAAA | 0.1 | 27001Academy | Descripción básica del documento |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Tabla de contenido**

[1. Objetivo, alcance y usuarios 2](#_Toc38349323)

[2. Autorizaciones y responsabilidades en la respuesta a los incidentes 2](#_Toc38349324)

[3. Comunicación 2](#_Toc38349325)

[4. Procedimientos para incidentes disruptivos 3](#_Toc38349326)

[4.1. Gestión de un incidente disruptivo 3](#_Toc38349327)

[4.1.1. Todos los empleados tienen la obligación de reportar incidentes 3](#_Toc38349328)

[4.1.2. Gestión de incidentes disruptivos 4](#_Toc38349329)

[4.1.3. Gerente de crisis 4](#_Toc38349330)

[4.2. Control y erradicación de un incidente 4](#_Toc38349331)

[4.2.1. Evacuación del edificio (independientemente del tipo de incidente) 4](#_Toc38349332)

[4.2.2. Incendio 5](#_Toc38349333)

[4.2.3. Interrupción del suministro eléctrico 5](#_Toc38349334)

[4.2.4. Terremoto 5](#_Toc38349335)

[4.2.5. Carta de amenaza 6](#_Toc38349336)

[4.2.6. Llamado de amenaza / amenaza de bomba 6](#_Toc38349337)

[4.2.7. Falla en las telecomunicaciones 7](#_Toc38349338)

[4.2.8. Falla en el sistema de información 7](#_Toc38349339)

[4.2.9. Ataque de código malicioso 7](#_Toc38349340)

[4.2.10. Violación de reglas internas o externas 8](#_Toc38349341)

[5. Gestión de registros guardados en base a este documento 8](#_Toc38349342)

[6. Validez y gestión de documentos 8](#_Toc38349343)

# Objetivo, alcance y usuarios

El objetivo de este Plan es asegurar la protección de la salud y de la seguridad de las personas ante el caso de un desastre o de otro incidente, como también contener el incidente. El objetivo es reducir al mínimo posible el daño sobre el negocio.

Este plan se aplica a todos los incidentes graves que amenazan con interrumpir cualquier actividad crítica dentro del alcance del SGSI [SGCN] por un período mayor al objetivo de tiempo de recuperación de cada actividad individual (en adelante, incidentes disruptivos).

Los usuarios de este documento son todos los empleados de [nombre de la organización].

# Autorizaciones y responsabilidades en la respuesta a los incidentes

|  |  |
| --- | --- |
| ***Función en la recuperación / cargo*** | ***Autorizaciones y responsabilidades*** |
| Cualquier empleado | Notificación del incidente a la unidad organizativa responsable |
| [cargo] o equipo en [nombre de la unidad organizativa] | Todos los pasos necesarios para resolver incidentes relacionados con tecnología de la información y de la comunicación |
| … | … |
| … | … |
| [cargo] | Comunicación con los medios públicos: esta persona tiene una autorización exclusiva para comunicarse con los medios públicos |
| [cargo] | Ayuda psicológica para los empleados |

# Comunicación

El siguiente cuadro detalla las responsabilidades para la comunicación (tanto envío como recepción de información y respuesta a solicitudes de información) con diversos tipos de partes involucradas:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | ***[Teléfono]*** | ***…*** | ***…*** | ***…*** | ***[Medios]*** |  |  |
| [Empleados] | \* |  |  |  |  |  |  |
| [Propietarios / accionistas] |  |  |  |  |  |  |  |
| [Familiares de empleados] |  |  |  |  |  |  |  |

\*\* FIN DE MUESTRA GRATIS \*\*

Para descargar la versión completa de este documento haga clic aquí: <https://advisera.com/27001academy/es/documentation/plan-de-respuesta-a-los-incidentes/>