\*\* VERSIÓN DE MUESTRA GRATIS \*\*

Gracias por descargar la vista previa gratuita del Paquete Premium de documentos sobre ISO 27001 e ISO 22301.

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

**Historial de modificaciones**

|  |  |  |  |
| --- | --- | --- | --- |
| **Fecha** | **Versión** | **Creado por** | **Descripción de la modificación** |
|  | 0.1 | Advisera | Descripción básica del documento |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Tabla de contenido

[1. Objetivo, alcance y usuarios 3](#_Toc130811565)

[2. Autorizaciones y responsabilidades en la respuesta a los incidentes 3](#_Toc130811566)

[3. Comunicación 3](#_Toc130811567)

[4. Procedimientos para incidentes disruptivos 4](#_Toc130811568)

[4.1. Gestión de un incidente disruptivo 4](#_Toc130811569)

[4.1.1. Obligación de reportar incidentes para cada empleado 4](#_Toc130811570)

[4.1.2. Gestión de incidentes disruptivos 4](#_Toc130811571)

[4.1.3. Gerente de crisis 5](#_Toc130811572)

[4.2. Control y erradicación de un incidente 5](#_Toc130811573)

[4.2.1. Evacuación del edificio (independientemente del tipo de incidente) 5](#_Toc130811574)

[4.2.2. Incendio 6](#_Toc130811575)

[4.2.3. Interrupción del suministro eléctrico 6](#_Toc130811576)

[4.2.4. Terremoto 6](#_Toc130811577)

[4.2.5. Carta de amenaza 7](#_Toc130811578)

[4.2.6. Llamado de amenaza / amenaza de bomba 7](#_Toc130811579)

[4.2.7. Falla en las telecomunicaciones 8](#_Toc130811580)

[4.2.8. Falla en el sistema de información 8](#_Toc130811581)

[4.2.9. Ataque de código malicioso 8](#_Toc130811582)

[4.2.10. Violación de reglas internas o externas 9](#_Toc130811583)

[5. Gestión de registros guardados en base a este documento 9](#_Toc130811584)

[6. Validez y gestión de documentos 9](#_Toc130811585)

# 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

|  |  |
| --- | --- |
| ***Rol en la recuperación / cargo*** | ***Autorizaciones y responsabilidades*** |
| Cualquier empleado | … |
| [cargo] o equipo en [nombre de la unidad organizativa] | … |
| [cargo] o equipo en [nombre de la unidad organizativa] | … |
| [cargo] o equipo en [nombre de la unidad organizativa] | … |
| [cargo] | … |
| [cargo] | … |

# 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]*** | ***[Reuniones]*** | ***[Correo electrónico]*** | ***[Conferencias de prensa]*** | ***[Medios]*** |  |  |
| [Empleados] |  |  |  |  |  |  |  |
| [Propietarios / accionistas] |  |  |  |  |  |  |  |
| [Familiares de empleados] |  |  |  |  |  |  |  |
| [Clientes] |  |  |  |  |  |  |  |
| [Medios públicos] |  |  |  |  |  |  |  |
| [Asociaciones] |  |  |  |  |  |  |  |
| [Servicios de emergencia] |  |  |  |  |  |  |  |
| [diversas autoridades públicas] |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

El procedimiento de comunicación es el siguiente:

1. Cualquier empleado que reciba una solicitud de comunicación o que desee iniciar la comunicación con las partes involucradas debe enviar esa solicitud a la persona responsable indicada en el cuadro anterior.
2. Una persona responsable debe estar de acuerdo con el [cargo] sobre el contenido de la comunicación. Siempre que sea posible, las plantillas de contenido de comunicación deben usarse como una forma de equilibrar la necesidad de información por parte de las partes interesadas y la prevención de rumores y desinformación.
3. Si la comunicación con los medios de comunicación y otras entidades externas incluye riesgos e impactos considerables, la decisión sobre esa comunicación debe ser documentada y formalmente autorizada por [cargo] antes de ser transmitida.
4. Luego de obtener la autorización correspondiente, la persona responsable le proporciona la información a la parte interesada.

La persona responsable indicada en el cuadro anterior tiene la responsabilidad de documentar cada pieza de comunicación con una parte involucrada.

# Procedimientos para incidentes disruptivos

## Gestión de un incidente disruptivo

### Obligación de reportar incidentes para cada empleado

Todos los empleados están obligados a informar cualquier incidente disruptivo de la siguiente manera:

* Todos los incidentes relacionados con tecnología de la información y de la comunicación son informados telefónicamente al [cargo o equipo de la unidad organizativa].
* Todos los demás incidentes son informados telefónicamente al [cargo o equipo de la unidad organizativa].

Cualquier otro evento o vulnerabilidad del sistema que todavía no se hubiera convertido en un incidente disruptivo debe ser informado de la misma forma.

Si un incidente demanda la intervención de la policía, de ambulancias o de los bomberos, la primera persona disponible debe llamar al [número de teléfono] y, desde allí, informar a la persona responsable de su unidad organizativa o al gerente de crisis.

En caso que ocurra un incidente, los empleados pueden comunicarse libremente sólo con sus familiares y con la policía, las ambulancias o los bomberos; mientras que cualquier otro tipo de comunicación se delega en el Gabinete de crisis.

### Gestión de incidentes disruptivos

La persona que recibe la información sobre el incidente debe evaluar si el incidente, o potencial incidente, es real o falso, y si se determina que es real, activa inmediatamente este Plan respetando los siguientes pasos:

* Comenzar a controlar y erradicar el incidente de acuerdo a lo detallado en las siguientes secciones del presente documento.
* Informar a todas las personas responsables sobre la ocurrencia del incidente dentro de su área de responsabilidad.
* Notificar a [cargo], que debe evaluar si es necesario alertar a alguna de las partes interesadas.
* Controla el estado del incidente y, si es necesario, informa a quien lo reportó y a los demás empleados involucrados, acerca del progreso en la gestión del incidente.

En caso que una persona no pueda controlar y/o erradicar el incidente, debe informarlo al gerente de crisis. La información que se envía al gerente de crisis debe incluir la naturaleza y alcance del incidente disruptivo, como también su potencial impacto.

La persona responsable de erradicar el incidente debe registrar en el Registro de incidentes todas las acciones tomadas.

### Gerente de crisis

El gerente de crisis debe supervisar el progreso en la gestión del incidente y el período de interrupción de las actividades individuales y debe evaluar el tiempo necesario para solucionar el incidente.

### Terremoto

Se evacua el edificio de acuerdo con el plan de evacuación del edificio.

|  |  |
| --- | --- |
| Gerente de crisis | * Notifica a la persona responsable de la unidad organizativa hacia la cual se dirige la amenaza. * No utiliza los puntos de encuentro habituales; escoge uno nuevo. * Si evalúa que la bomba realmente puede detonarse, ordena la evacuación; el punto de encuentro debe estar alejado 300 metros como mínimo. * Informa a las personas responsables de la evacuación y al Gabinete de apoyo de crisis la ubicación del nuevo punto de encuentro. * En caso de una explosión, toma una decisión para alejar de la zona afectada, lo antes posible, a los heridos. |

### …

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

Si ha decidido que el Paquete Premium de documentos sobre ISO 27001 e ISO 22301 es la mejor elección para su compañía, consulte la siguiente tabla para elegir el paquete de documentos con el nivel de soporte experto adecuado.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Paquete de documentos con apoyo de un experto** | **Paquete de documentos con ampliación de soporte** | **Paquete de documentos superior** |
|  | **US $997** | **US $1497** | **US $2497** |
| **64 plantillas de documentos que cumplen con ISO 27001** | **🗸** | **🗸** | **🗸** |
| **Acceso a tutoriales en video (en inglés)** | **🗸** | **🗸** | **🗸** |
| **Plantillas de documentos actualizadas a la versión ISO 27001:2022** | **🗸** | **🗸** | **🗸** |
| **Herramienta de Análisis de Brecha en ISO 27001** | **🗸** | **🗸** | **🗸** |
| **Soporte mediante correo electrónico** | 10 preguntas por mes | Ilimitado | Ilimitado |
| **Asistencia personalizada con un experto en ISO 27001 e ISO 22301** | 1 hora | 5 horas | 15 horas |
| **Revisión de expertos (documentos completos)** | 1 documento | 5 documentos | 15 documentos |
| **Formación en concienciación sobre seguridad (en inglés)** | **X** | 20 usuarios | 50 usuarios |
| **Revisión previa a la auditoría** | **X** | **🗸** | **🗸** |
|  | [**SOLICÍTELO AHORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718233&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=es?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-iso-22301-templates&utm_term=toolkit-with-expert-support&utm_content=lang-es) | [**SOLICÍTELO AHORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718234&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=es?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-iso-22301-templates&utm_term=toolkit-with-extended-support&utm_content=lang-es) | [**SOLICÍTELO AHORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718235&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=es?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-iso-22301-templates&utm_term=toolkit-with-power-support&utm_content=lang-es) |
|  | (haga clic en el siguiente enlace presionando CTRL+clic) | | |