

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

Commented [AES1]: Para saber cómo completar este documento, y ver ejemplos reales de lo que necesita escribir, vea este tutorial en vídeo: "How to Write a Business Continuity Plan According to ISO 22301".

Para acceder al tutorial: en su bandeja de entrada, busque el correo electrónico que recibió en el momento de la compra. Allí, verá un enlace y una contraseña que le permitirán acceder al tutorial en vídeo.

TABLA DE CONTENIDO

1. OBJETIVO, ALCANCE Y USUARIOS.....	3
2. AUTORIZACIONES Y RESPONSABILIDADES EN LA RESPUESTA A LOS INCIDENTES.....	3
3. COMUNICACIÓN.....	3
4. PROCEDIMIENTOS PARA INCIDENTES DISRUPTIVOS.....	4
4.1. GESTIÓN DE UN INCIDENTE DISRUPTIVO.....	4
4.1.1. <i>Obligación de reportar incidentes para cada empleado.....</i>	4
4.1.2. <i>Gestión de incidentes disruptivos.....</i>	4
4.1.3. <i>Gerente de crisis.....</i>	5
4.2. CONTROL Y ERRADICACIÓN DE UN INCIDENTE.....	5
4.2.1. <i>Evacuación del edificio (independientemente del tipo de incidente).....</i>	5
4.2.2. <i>Incendio.....</i>	6
4.2.3. <i>Interrupción del suministro eléctrico.....</i>	6
4.2.4. <i>Terremoto.....</i>	6
4.2.5. <i>Carta de amenaza.....</i>	7
4.2.6. <i>Llamado de amenaza / amenaza de bomba.....</i>	7
4.2.7. <i>Falla en las telecomunicaciones.....</i>	8
4.2.8. <i>Falla en el sistema de información.....</i>	8
4.2.9. <i>Ataque de código malicioso.....</i>	8
4.2.10. <i>Violación de reglas internas o externas.....</i>	9
5. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO.....	9
6. VALIDEZ Y GESTIÓN DE DOCUMENTOS.....	9

1. 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].

Commented [AES2]: Se debe insertar esta leyenda en lugar de SGSI en caso que el proyecto involucre sólo al SGCN.

Commented [AES3]: Incluya el nombre de su organización.

2. Autorizaciones y responsabilidades en la respuesta a los incidentes

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

Commented [AES4]: Para obtener más información sobre este tema, lea este artículo:

Commented [AES5]: Ej.: jefe del departamento de TI.

Commented [AES6]: Ej.: oficial de operaciones.

Commented [AES7]: Debe ser la persona designada en el Plan

Commented [AES8]: Para obtener más información sobre este tema, lea este artículo:

Commented [AES9]: Debe ser la persona designada en el Plan

Commented [AES10]: Debe ser nombrado por el gerente /

Commented [AES11]: Para obtener más información sobre este tema, lea este artículo:

Commented [AES12]: Se debe ampliar esta sección con

Commented [AES13]: Copiar responsabilidades de la Estrategia

3. 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:

[Empleados]							
[Propietarios / accionistas]							
[Familiares de empleados]							

--	--	--	--	--	--	--	--

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. La persona responsable debe estar de acuerdo con el [redacted] sobre el contenido de la comunicación. Siempre que sea posible, la solicitud de contenido de comunicación debe estar en una forma de escribir la necesidad de información por parte de la parte interesada y la provisión de misma y disponibilidad.
3. Si la comunicación con las partes de comunicación y otras entidades externas incluye riesgo o impacto considerable, la persona responsable debe ser documentada y formalmente autorizada por el jefe antes de su realización.
4. Luego de obtener la autorización correspondiente, la persona responsable le proporciona la información a la parte interesada.

Commented [AES14]: Debe ser la persona designada en el Plan

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

4. Procedimientos para incidentes disruptivos

Commented [AES15]: Incluir aqui todos los incidentes

4.1. Gestión de un incidente disruptivo

4.1.1. Obligación de reportar incidentes para cada empleado

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

1. Todos los incidentes disruptivos con respecto de la información o de la comunicación de [redacted] deben ser reportados al jefe o a quien de la unidad responsable.
2. Todos los demás incidentes con información confidencial o a cargo de la unidad responsable.

Commented [AES16]: Si este tema ya está reglamentado por el

Commented [AES17]: Ej.: jefe del departamento de TI.

Commented [AES18]: Ej.: oficial de operaciones.

Además, una vez que se ha informado de un incidente disruptivo, el [redacted] debe ser informado de la misma forma.

Commented [AES19]: Si este tema ya está reglamentado por el

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.

4.1.2. 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 todos los gerentes responsables sobre la existencia del incidente dentro de su área de responsabilidad.
- Notificar a [AES20] con el fin de evaluar y/o erradicar dentro o después de las partes afectadas.
- Controlar el estado del incidente y, si es necesario, informar a todos los gerentes y/o áreas involucradas involucradas, acerca del progreso en la gestión del incidente.

Commented [AES20]: Ej. gerente de continuidad de negocio, gerente de TI, etc.

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.

4.1.3. 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.

En el tiempo necesario para solucionar el incidente se debe que el objetivo de tiempo de recuperación de una actividad particular, se debe activar el plan de recuperación para la actividad afectada. En caso que el gerente de crisis debe comunicarse con los gerentes de recuperación, según activado en planes de recuperación.

4.2. Control y erradicación de un incidente

Commented [AES21]: Este capítulo solamente proporciona información de referencia para el plan de continuidad de negocio.

4.2.1. Evacuación del edificio (independientemente del tipo de incidente)

Se evacua el edificio y se dirige al personal hacia los puntos de encuentro especificados en la Lista de ubicaciones para continuidad de negocio, incluida como apéndice al Plan de continuidad de negocio.

Gerente de crisis	<ul style="list-style-type: none"> • En caso que esté en riesgo la vida o la salud de las personas, emite una orden de evacuación. • Si el punto de encuentro es un punto designado, como se describe en el plan de continuidad de negocio, se debe activar el plan de recuperación para la actividad afectada, según activado en planes de recuperación, etc. • En caso de una emergencia real, como un incendio, debe la persona responsable del punto de encuentro dentro de un punto de encuentro de la oficina, según activado en planes de recuperación, etc.
Personas	<ul style="list-style-type: none"> • Dirige la evacuación hacia el punto de encuentro.

responsables de ejecutar la evacuación	<ul style="list-style-type: none"> • Verificar que todos los edificios estén en un estado seguro de la evacuación, salir de los edificios y cerrar las puertas con llave. • En caso que alguien no haya podido salir del edificio, la oficina o cualquier otro edificio del centro de emergencia.
Todos los empleados	<ul style="list-style-type: none"> • Evacuan según los planes de evacuación para su edificio. • Siguen las instrucciones suministradas por las personas responsables de dirigir la evacuación. • No utilizan ascensores durante la evacuación. • Al evacuar, solamente llevan un bolso de mano y artículos, no llevan ningún otro elemento. • Reúnen a todas y a otras personas, si necesitan ayuda.
Gabinete de apoyo de crisis	<ul style="list-style-type: none"> • Cuando la gente se ha reunido en el punto de encuentro, lleva un registro de todas las personas presentes y las que faltan.

4.2.2. Incendio

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

Gerente de crisis	<ul style="list-style-type: none"> • En caso que esté en riesgo la vida o la salud de las personas, el gerente de crisis emite una orden de evacuación. • Encarga las medidas para disminuir el daño a otras áreas, a menos que esto represente un riesgo para la persona.
-------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

4.2.3. Interrupción del suministro eléctrico

Gabinete de apoyo de crisis	<ul style="list-style-type: none"> • Establece la causa de la interrupción; es originada por el cableado o por el distribuidor de electricidad.
[Cargo] o el equipo designado	<ul style="list-style-type: none"> • Soluciona el problema junto con el distribuidor de electricidad.
Todos los empleados	<ul style="list-style-type: none"> • Cumpliendo con los planes de emergencia, acceden con los medios alternativos para operar actividades, en el caso de electricidad.
Equipos de soporte de emergencia (Ej. IT)	<ul style="list-style-type: none"> • Supervisan los dispositivos (Ej. Documentación de sistemas alternativos) en caso de emergencia.

Commented [AES22]: Ej. analista de instalaciones, técnico de

4.2.4. Terremoto

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

Todos los	<ul style="list-style-type: none"> • Buscan refugio bajo el marco de una puerta, cerca de una pared interior de
-----------	--------------------------------------------------------------------------------------------------------------------------------

empleados	<p>apoyo, o debajo de un escritorio.</p> <ul style="list-style-type: none"> 1. No utilizar los ascensores. 2. No correr hacia el exterior del edificio hasta que termine el terremoto. 3. Una vez que el terremoto ha finalizado, mantener calmado a otras personas antes que se haga más daño a la persona herself. 4. Si una persona exhibe la incomodidad, proporcionar asistencia al plan de emergencia.
Gerente de crisis	<ul style="list-style-type: none"> • En caso que esté en riesgo la vida o la salud de las personas, ordena la evacuación del edificio una vez que haya terminado el terremoto.
Gabinete de apoyo de crisis	<ul style="list-style-type: none"> • Apaga todos los servicios: gas, electricidad, calefacción, ventilación, suministro de agua. • [Redacción de edificio y demás temas...]

4.2.5. Carta de amenaza

Todos los empleados	<ul style="list-style-type: none"> • Si reciben una carta sospechosa, no la abren, la sostienen sólo por sus bordes externos. 1. No utilizar los ascensores. 2. Informar al [Redacción] 3. Proporcionar copia de la carta a [Redacción]
[Cargo] o el equipo designado	<ul style="list-style-type: none"> • Notifica a la policía a través del [número de teléfono]. 1. Notifica al supervisor del empleado que exhibe la carta. 2. Operar las medidas requeridas por la policía.

Commented [AES23]: Ej.: oficial de seguridad.

Commented [AES24]: Ej.: oficial de seguridad.

Commented [AES25]: Ej.: oficial de seguridad.

4.2.6. Llamado de amenaza / amenaza de bomba

Todos los empleados	<ul style="list-style-type: none"> • Si reciben una llamada de amenaza, anotan la hora exacta y el número de teléfono que llamó. 1. Mantener las personas alejadas de la persona que llama. 2. Esperar que quien llama haga lo más posible, sin interrupciones: <ul style="list-style-type: none"> - Mantener tranquilo a la persona que llama. - Responder las preguntas. Mantener que se comprenden lo que dijo. - Si una persona parece alarmada, poner la llamada en silencio y pedir a otra persona que tome el teléfono. - Responder cada solicitud recibida por la persona que llama. 3. Si uno de sus miembros de familia, le hacen las siguientes preguntas a la persona que llama: <ul style="list-style-type: none"> - ¿Dónde está la bomba? ¿Cuándo? - ¿Es posible desactivarla? ¿Cómo? - ¿Dónde está el detonador? - ¿Cómo es? - ¿Por qué fue colocado? ¿Cuál es la amenaza? - ¿Quién llamó? ¿Puede decir su nombre?
---------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<ul style="list-style-type: none"> • Alerte a los puntos de contacto de la oficina sobre el estado de la amenaza. • Alerte a los puntos de contacto de la oficina sobre el estado de la amenaza. • Notifica a los puntos de contacto de la oficina sobre el estado de la amenaza. • Se asocia a los puntos de contacto de la oficina sobre el estado de la amenaza.
Gerente de crisis	<ul style="list-style-type: none"> • Notifica a la persona responsable de la unidad organizativa hacia la cual se dirige la amenaza. • Se asocia a los puntos de contacto de la oficina sobre el estado de la amenaza. • Se asocia a los puntos de contacto de la oficina sobre el estado de la amenaza. • Se asocia a los puntos de contacto de la oficina sobre el estado de la amenaza. • Se asocia a los puntos de contacto de la oficina sobre el estado de la amenaza. • Se asocia a los puntos de contacto de la oficina sobre el estado de la amenaza.

4.2.7. Falla en las telecomunicaciones

Empleado del [nombre del departamento]	<ul style="list-style-type: none"> • Cualquier empleado recibe información sobre la falla. • Se asocia a los puntos de contacto de la oficina sobre el estado de la amenaza.
Empleados - usuarios de servicios de comunicación	<ul style="list-style-type: none"> • Utilizan vías de comunicación alternativas.

Commented [AES26]: Estas son responsabilidades del [nombre del departamento] de [nombre de la organización].

4.2.8. Falla en el sistema de información

Empleado del [nombre del departamento]	<ul style="list-style-type: none"> • Cualquier empleado recibe información sobre el incidente. • Se asocia a los puntos de contacto de la oficina sobre el estado de la amenaza. • Se asocia a los puntos de contacto de la oficina sobre el estado de la amenaza.
Gerente de crisis	<ul style="list-style-type: none"> • Se asesora sobre todos los servicios importantes, evalúa la gravedad del incidente.
Todos los empleados	<ul style="list-style-type: none"> • Si es posible, realizan procedimientos alternativos para llevar adelante las actividades.

Commented [AES27]: Estas son responsabilidades del [nombre del departamento] de [nombre de la organización].

4.2.9. Ataque de código malicioso

Empleado del [nombre del departamento]	<ul style="list-style-type: none"> • Cualquier empleado recibe información sobre el incidente. • Se asocia a los puntos de contacto de la oficina sobre el estado de la amenaza. • Se asocia a los puntos de contacto de la oficina sobre el estado de la amenaza. • Se asocia a los puntos de contacto de la oficina sobre el estado de la amenaza.
----------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Commented [AES28]: Estas son responsabilidades del [nombre del departamento] de [nombre de la organización].

	<ul style="list-style-type: none"> • Desconectan físicamente de la red cualquier ordenador infectado, desactivan las redes inalámbricas, de Bluetooth, etc. • No pagan los dispositivos de red o conectados, como es el caso de los dispositivos de [redacción]
Todos los empleados	
Empleados del [nombre del departamento]	<ul style="list-style-type: none"> • Si el ordenador todavía no ha sido desconectado de la red, evalúa si lo desconecta para evitar mayor infección. • Desactiva todos los dispositivos inalámbricos del ordenador. • Limpia cualquier teclado o mouse conectado, para los dispositivos, cables o de cualquier otro tipo de cable, incluidos o cables de audio, incluidos en el equipo de trabajo, incluidos o cables de audio, incluidos en el equipo de trabajo, incluidos o cables de audio, incluidos en el equipo de trabajo. • Limpia físicamente cables de tipo de cable, incluidos o cables de audio, incluidos en el equipo de trabajo, incluidos o cables de audio, incluidos en el equipo de trabajo. • Limpia físicamente cables de tipo de cable, incluidos o cables de audio, incluidos en el equipo de trabajo, incluidos o cables de audio, incluidos en el equipo de trabajo. • Limpia físicamente cables de tipo de cable, incluidos o cables de audio, incluidos en el equipo de trabajo, incluidos o cables de audio, incluidos en el equipo de trabajo.

Commented [AES29]: Estas son responsabilidades del [redacción]

Commented [AES30]: Estas son responsabilidades del [redacción]

4.2.10. Violación de reglas internas o externas

	<ul style="list-style-type: none"> • El procedimiento se realiza de acuerdo a lo establecido en los procedimientos disciplinarios regulados por las leyes laborales y por la propia organización.
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

5. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del acceso	Acciones para la protección del registro	Fecha de revisión
Registro de incidentes	Carpeta compartida en Intranet	[redacción]	[redacción]	[redacción]

Commented [AES31]: Inserte los datos en esta columna para [redacción]

Commented [AES32]: Ej.: gerente de incidentes, analista de [redacción]

Commented [AES33]: Ej. gerente de incidentes, oficial de [redacción]

Solamente el [cargo] puede permitir el acceso a los registros a otros empleados.

6. Validez y gestión de documentos

Este documento es válido desde el [fecha].

Este documento, junto con todos los materiales adicionales, es archivado de la siguiente forma:

- El documento en papel se archiva en las siguientes ubicaciones: Centro de crisis y todas las ubicaciones alternativas para actividades

- [redacción]

Commented [AES34]: Archivar los documentos de forma que [redacción]

[nombre de la organización]

[nivel de confidencialidad]

El propósito de este documento es [cargar], que debe incluir, y no limitar, ejemplos de documentos por la norma [AES35].

Commented [AES35]: Esto es sólo una recomendación; ajustar [AES35].

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de incidentes no contemplados en el presente documento.
- Todos los casos descritos en el presente documento son factibles en situaciones reales.
- Tiempo de respuesta a los incidentes.

[cargo]

[nombre]

[firma]

Commented [AES36]: Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.