Apéndice 1 – Plan de respuesta a los incidentes

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.

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

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].

2. Autorizaciones y responsabilidades en la respuesta a los incidentes

[redacted]	[redacted]
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
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

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:

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

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.

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

[redacted]

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

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

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

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

[redacted]

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

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

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

[redacted]

Commented [AES12]: Se debe ampliar esta sección con [redacted]

Commented [AES13]: Copiar responsabilidades de la Estrategia [redacted]

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. [illegible]
3. [illegible]
4. [illegible]

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

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 aquí todos los incidentes [illegible]

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:

- [illegible]
- [illegible]

[illegible]

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

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

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

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

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.
- [illegible]
- [illegible]
- [illegible]

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

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.

[illegible]

4.2. Control y erradicación de un incidente

Commented [AES21]: Este capítulo solamente proporciona [illegible]

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	• En caso que esté en riesgo la vida o la salud de las personas, emite una orden de evacuación. • [illegible] • [illegible]
Personas	• Dirige la evacuación hacia el punto de encuentro.

responsables de ejecutar la evacuación	• [illegible] • [illegible]
Todos los empleados	• Evacuan según los planes de evacuación para su edificio. • [illegible] • [illegible] • [illegible] • [illegible]
Gabinete de apoyo de crisis	• 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	• En caso que esté en riesgo la vida o la salud de las personas, el gerente de crisis emite una orden de evacuación. • [illegible]

4.2.3. Interrupción del suministro eléctrico

Gabinete de apoyo de crisis	• Establece la causa de la interrupción; es originada por el cableado o por el distribuidor de electricidad.
[Cargo] o el equipo designado	• Soluciona el problema junto con el distribuidor de electricidad.
[illegible]	• [illegible]
[illegible]	• [illegible]

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

4.2.4. Terremoto

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

Todos los	• Buscan refugio bajo el marco de una puerta, cerca de una pared interior de

empleados	apoyo, o debajo de un escritorio. • [illegible] • [illegible] • [illegible] • [illegible]
Gerente de crisis	• 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	• Apaga todos los servicios: gas, electricidad, calefacción, ventilación, suministro de agua. • [illegible]

4.2.5. Carta de amenaza

Todos los empleados	• Si reciben una carta sospechosa, no la abren, la sostienen sólo por sus bordes externos. • [illegible] • [illegible] • [illegible]
[Cargo] o el equipo designado	• Notifica a la policía a través del [número de teléfono]. • [illegible] • [illegible]

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	• Si reciben una llamada de amenaza, anotan la hora exacta y el número de teléfono que llamó.
	• [illegible]
	• [illegible]
	  ○ [illegible]
	  ○ [illegible]
	  ○ [illegible]
	  ○ [illegible]
	• [illegible]
	  ○ [illegible]
	  ○ [illegible]
	  ○ [illegible]
	  ○ [illegible]
	  ○ [illegible]
	  ○ [illegible]

	• [redacted]
Gerente de crisis	• Notifica a la persona responsable de la unidad organizativa hacia la cual se dirige la amenaza. • [redacted]

4.2.7. Falla en las telecomunicaciones

Empleado del [nombre del departamento]	• Cualquier empleado recibe información sobre la falla. • [redacted]
Empleados - usuarios de servicios de comunicación	• Utilizan vías de comunicación alternativas.

Commented [AES26]: Estas son responsabilidades del [redacted]

4.2.8. Falla en el sistema de información

Empleado del [nombre del departamento]	• Cualquier empleado recibe información sobre el incidente. • [redacted]
Gerente de crisis	• Se asesora sobre todos los servicios importantes, evalúa la gravedad del incidente.
Todos los empleados	• Si es posible, realizan procedimientos alternativos para llevar adelante las actividades.

Commented [AES27]: Estas son responsabilidades del [redacted]

4.2.9. Ataque de código malicioso

Empleado del [nombre del departamento]	• Cualquier empleado recibe información sobre el incidente. • [redacted]

Commented [AES28]: Estas son responsabilidades del [redacted]

	• [redacted]
Todos los empleados	• Desconectan físicamente de la red cualquier ordenador infectado, desactivan las redes inalámbricas, de Bluetooth, etc. • [redacted]
Empleados del [nombre del departamento]	• Si el ordenador todavía no ha sido desconectado de la red, evalúa si lo desconecta para evitar mayor infección. • [redacted]

Commented [AES29]: Estas son responsabilidades del

Commented [AES30]: Estas son responsabilidades del

4.2.10. Violación de reglas internas o externas

[redacted]	• 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*	[redacted]	[redacted]	[redacted]
Registro de incidentes	Carpeta compartida en Intranet	[redacted]	[redacted]	[redacted]

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

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

Commented [AES33]: Ej. gerente de Incidentes, oficial de

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
- [redacted]

Commented [AES34]: Archivar los documentos de forma que

El propietario de este documento es el [cargo], que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

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

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.
- Si los pasos detallados 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.