Aarón Espinosa Asencio

PLAN DE RESPUESTA A INCIDENTES

Your delivery!

Índice

Introducción

Es importante tener claras las medidas que implantaremos en cuanto a **incidentes de ciberseguridad**, por lo que hay que preparar un correcto **plan de acción** que nos indique la mejor manera de responder ante dichos incidentes.
En nuestra empresa en la que basaremos el plan de respuestas ***your delivery!***, existen varios posibles incidentes que pueden darse en determinadas circunstancias, entre los más importantes debido a la naturaleza de la empresa (empresa de reparto de comida a domicilio) tenemos:

- Login no autorizado y fallido
- Backup fallido por corte de luz
- Fallo datáfono en pago a domicilio
- Inundación del local

En este documento se detallará el procedimiento mediante el cual se actuará en caso de detectar alguno de estos incidentes basándonos en la guía para respuestas a incidentes de **INCIBE**.

Este documento se revisará semestralmente y esta sujeto a cambios si esto implica la mejora de los sistemas de detección y de respuesta a incidentes.

Descripción de los incidentes

Incidente	Descripción
Login no autorizado y/o fallido	Intento de acceso al sistema por alguna persona sin la correspondiente autorización, si se produce reiteradamente y no se detecta a tiempo puede llevar a un login exitoso en el futuro, este sería el peor de los escenarios posibles, ya que se tendría acceso a todos los datos de los usuarios así como su información de pago.
Corte de luz	Fallo en el sistema eléctrico por un factor ya sea externo (fuertes lluvias, terremoto) o interno (fallo de generadores), interrumpiría el correcto funcionamiento de la empresa.
Fallo datáfono en pago a domicilio	El cliente no puede pagar a la hora de recibir el pedido en casa debido a un fallo con el dispositivo de cobro, ya sea por falta de señal o fallo del mismo dispositivo, esto puede llevar a perder dinero.
Inundación del local	Inundación del establecimiento por factores meteorológicos, puede desencadenar más problemas como cortocircuitos, destrozo de material e incluso muertes en los peores casos.

¿Cómo detectarlos?

Login no autorizado y fallido

La persona encargada de detectar y tratar este incidente es el administrador de sistemas de la empresa, quien determinará revisando frecuentemente los logs y monitorizando el sistema si se ha intentado acceder al sistema sin autorización con el fin de que no se produzca reiteradamente y se llegue a acceder.

Corte de luz

Es evidente que a la hora de detectar un corte de luz es tan fácil como ver que no existe corriente en ningún lugar del establecimiento.
Lo primero que se deberá determinar es si es debido a un fallo de los generadores o por un factor externo como algún desastre natural.

En el caso de ser un fallo de los generadores, la persona encargada de determinar si esto es así es el encargado de mantenimiento, en el caso de que verifique que funcionan correctamente y sepa que es debido a un agente externo.

Fallo datáfono en pago a domicilio

Cuando el cliente reciba su pedido, si ha seleccionado la opción de pago con tarjeta, el repartidor llevará consigo un datáfono y será el encargado de reportar cualquier incidente derivado del uso de este.

Inundación del local

En las instalaciones se cuenta con sensores que detectan la humedad, si se detecta niveles altos por encima de lo habitual se alertará automáticamente al encargado de mantenimiento.

Categorización de los incidentes

En función del daño causado por los incidentes, se establecen unas categorías que indican la peligrosidad de este.

Login no autorizado y/o fallido

Hecho	Gravedad
Login realizado	**Máxima**
Único intento de login	**Baja**
Intentos repetidos de login	**Media**

Corte de luz

Hecho	Gravedad
Más de 3h duración	**Máxima**
Duración < 1h	**Baja**
Cortes breves pero frecuentes	**Media**

Fallo datáfono

Hecho	Gravedad
El cliente no dispone de otro medio de pago y no puede pagar	**Máxima**
El cliente consigue pagar mediante otro medio	**Media**

Inundación del local

Hecho	Gravedad
Imposibilidad de funcionamiento de la empresa	**Máxima**
Pocos o ningún daño material	**Baja**
Daños materiales significativos (Dispositivos, datáfonos…)	**Media**

Respuesta a los incidentes

Login no autorizado y fallido

- El administrador de sistemas enviará un circular a los empleados de la organización vía email para notificarlos y asegurarse de que no fue nadie del interior de la empresa.
- En el caso de que hayan conseguido entrar en el sistema mediante el login y se haya identificado, cesará la actividad de la empresa hasta que no se haya evaluado el alcance del mismo y se haya restablecido todo y verificado que no existen puertas traseras.
- Se documentará todo el proceso de detección hasta la resolución del incidente.
- Se aplicarán las medidas correctivas adecuadas, en caso de necesitar apoyo se recurrirá a ***Incibe***.

Medidas de ciberresilencia tras la Autoevaluación

ANTICIPAR

Objetivo	Medida
Establecer los requisitos de Ciberresiliencia para soportar los servicios esenciales.	Identificar, documentar y revisar los requisitos de ciberresiliencia del servicio esencial identificado. Actualizar la documentación asociada a la política de ciberseguridad.
Colaborar con entidades públicas o privadas en materia de ciberresiliencia.	Establecer, formalizar y revisar acuerdos de ayuda mutua, cooperación o intercambio de información con entidades privadas o públicas, para garantizar la colaboración mutua en caso de un ciberataque.
Estimar el Tiempo Máximo Tolerable de caída (MTD) o tiempo que puede estar caído un servicio esencial antes de que se produzcan efectos no aceptables.	Establecer criterios y procedimientos para estimar los periodos máximos tolerables de interrupción para cada proceso y actividad que soporte el servicio esencial para el cual estamos haciendo la encuesta. Documentar, revisar y gestionar el procedimiento para estimar tiempo máximo tolerable de interrupción para el servicio esencial.
Existe un procedimiento específico para implementar las actividades de gestión de riesgos.	Establecer un procedimiento de gestión del riesgos relativos a la provisión del servicio esencial basado en referencias como CCNSTIC 882 de Análisis de Riesgos para Entidades Locales, o el Modelo de Análisis de Riesgos Ligero de Ciberseguridad en Sistemas de Control Industrial (ARLI-CIB) de INCIBE-CERT
Identificar las necesidades de formación en Ciberseguridad para los servicios esenciales.	Destinar tiempo y dedicar recursos para identificar las necesidades de formación en Ciberseguridad de la organización. Actualizar periódicamente las necesidades de formación en Ciberseguridad para adecuarlas al nivel de seguridad necesario, a las nuevas amenazas y a los distintos perfiles profesionales de la empresa.

RESISTIR

Objetivo	Medida
Categorizar y priorizar las vulnerabilidades.	**Categorizar y priorizar las vulnerabilidades para reportarlas a los responsables.** **Documentar y actualizar un procedimiento de categorización y priorización de vulnerabilidades.**
Establecer y mantener un repositorio actualizado de vulnerabilidades.	**Establecer un repositorio de vulnerabilidades con información del ciclo de vida de las mismas. Dicho repositorio debe contener información básica como:** **• Identificador único para referencia interna de la vulnerabilidad en la organización.** **• Descripción de la vulnerabilidad.** **• Fecha de ingreso en el repositorio.** **• Referencias a la fuente de la vulnerabilidad.** **• Importancia de la vulnerabilidad para la organización (crítica, moderada, etc.)** **• Personas o equipos asignados para analizarla y solucionarla.** **• Registro de las acciones de resolución tomadas para disminuir o eliminar la vulnerabilidad.**

RECUPERAR

Objetivo	Medida
Establecer un proceso para estimar la capacidad de respuesta y recuperación de los ciberincidentes.	**Establecer un procedimiento para estimar el tiempo medio de respuesta a un ciberincidente y el uso de recursos en horas de técnicos en su resolución.** **Documentar, actualizar y verificar el procedimiento para estimar el tiempo medio de resolución.**
Evaluar la respuesta de la organización desde la interrupción del servicio esencial hasta su recuperación a un nivel mínimo aceptable.	**Establecer los mecanismos necesarios (tecnológicos, logísticos y físicos) para valorar el tiempo necesario para que el servicio esencial vuelva a estar disponible a un nivel mínimo tras el evento de interrupción. Esto se puede realizar, por ejemplo, apoyándose en los ejercicios de simulación de interrupción del servicio esencial.**
Evaluar la respuesta de la organización desde la interrupción del servicio esencial hasta su recuperación completa y funcionamiento normal.	**Establecer los mecanismos necesarios (tecnológicos, logísticos y físicos) que permitan valorar cómo se ha conseguido recuperar la normalidad del servicio esencial para que éste vuelva a estar disponible de forma completa en el menor tiempo posible pasado el evento de interrupción. Una manera constructiva consiste en registrar los tiempos cuando están ocurriendo los hitos de: interrupción, recuperación mínima del servicio, y recuperación completa del servicio.**
Identificar y priorizar las dependencias externas relacionadas con la provisión del servicio esencial.	**Establecer unos criterios para identificar y priorizar las dependencias externas. Mantener los criterios y prioridades documentados, actualizados y revisarlos periódicamente.**

EVOLUCIONAR

Objetivo	Medida
Comunicar la estrategia de continuidad a toda la organización.	**Establecer mecanismos eficaces de comunicación externa a través de los canales habilitados.** **Crear las buenas prácticas para comunicar los ciberincidentes.**

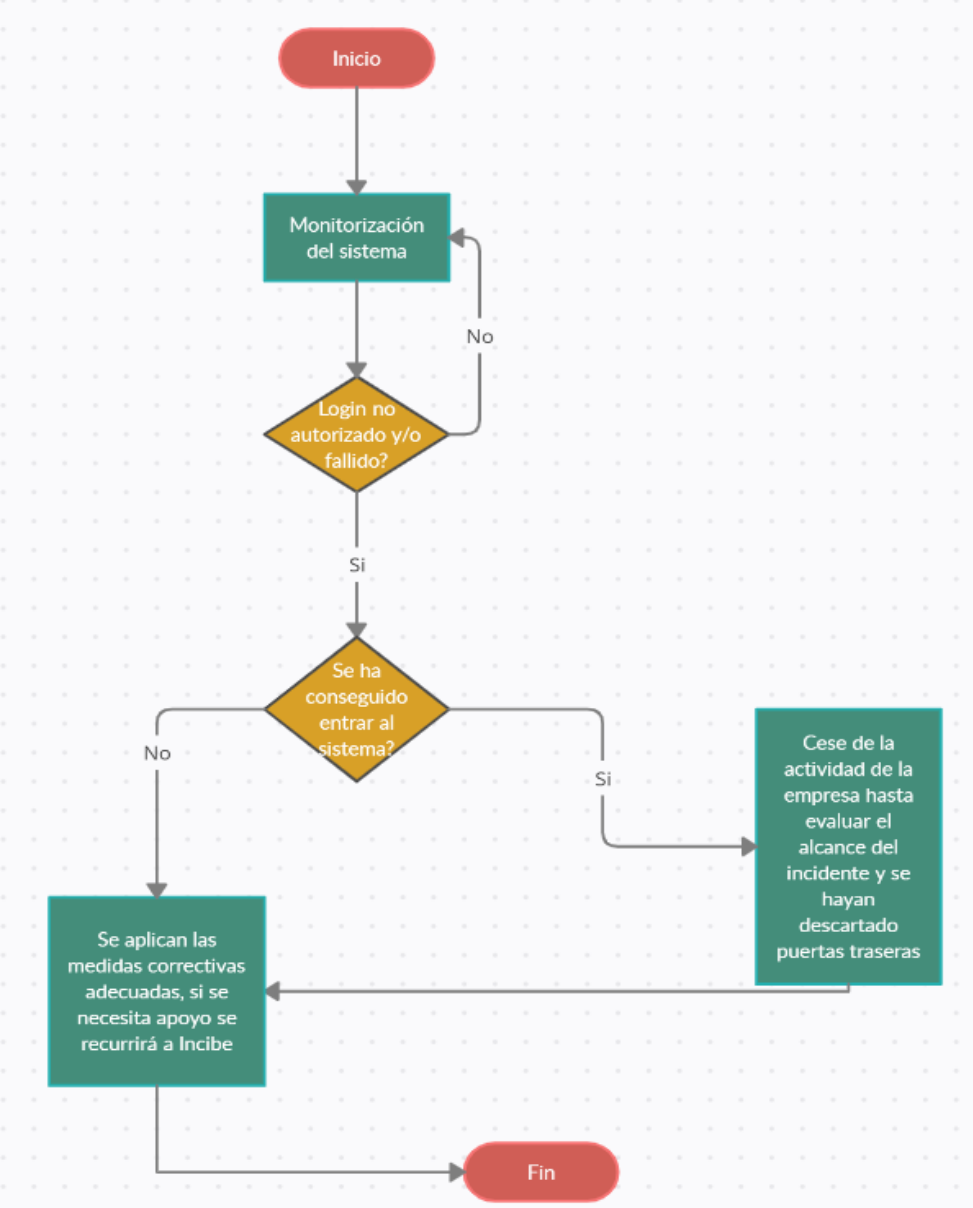


Diagrama de resolución del incidente

Corte de luz

- En el caso de que haya sido provocado por los generadores propios de la empresa, el encargado de mantenimiento llamará al número de soporte técnico de los generadores para que resuelvan el problema o reemplacen si es necesario los generadores, hasta entonces se usarán varios SAI (sistema de alimentación ininterrumpida) para alimentar los dispositivos indispensables para el funcionamiento de la empresa (neveras, congeladores…) durante el tiempo que dure la avería o fallo.
- En el caso de que haya sido debido a un factor externo a la empresa, se hará uso de los generadores propios para operar mientras tanto.

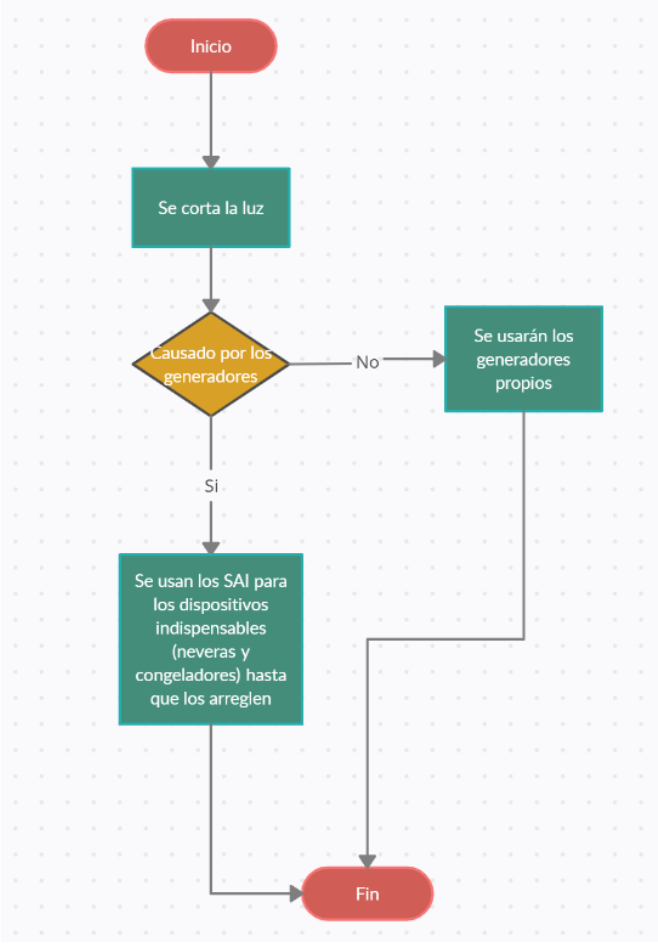


Diagrama de resolución del incidente

Fallo datáfono en pago a domicilio

- En el mejor de los casos, el cliente podrá encontrar otro método de pago (efectivo, bizum…) para pagar.
- Si el cliente no dispone de otro medio para pagar, tenemos el compromiso de proporcionar la comida sin ningún costo ya que el fallo es ajeno a ellos.
- En cualquier caso, si fallase el datáfono, se detallará un informe por parte del repartidor especificando las condiciones en las que falló y la causa o posible causa de por qué puede haber sido, además de contactar con soporte técnico de la empresa que los fabrica para reportar la falla.

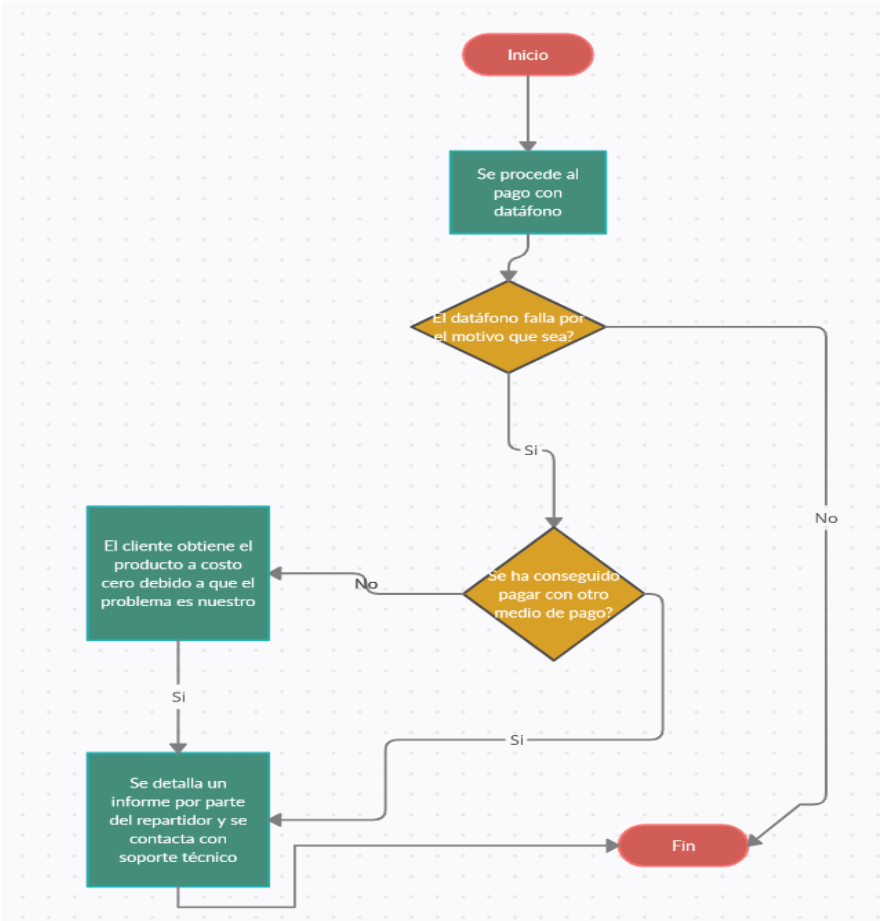
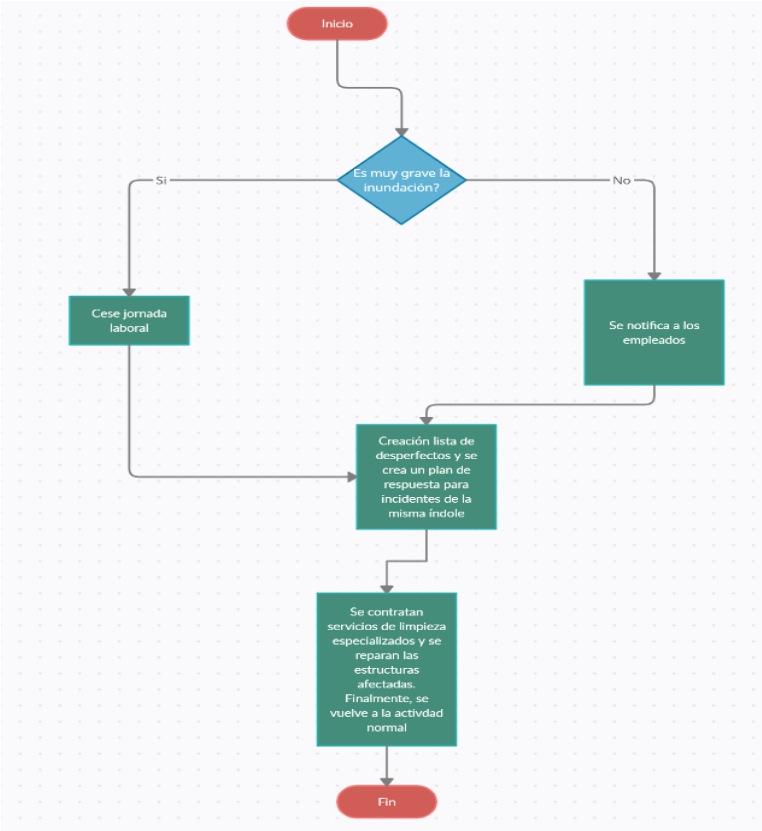


Diagrama de resolución del incidente

Inundación del local

- En primer lugar, se notificaría según la gravedad a los empleados para cesar las jornadas laborales hasta que no se solucione el problema, esta notificación deberá emitirla el encargado de mantenimiento que sería previamente avisado por los sistemas de humedad de las instalaciones.
- Se hará una lista de los desperfectos causados para hacer una estimación del costo de reparación o reemplazo del material.
- Se establecerá un plan de respuesta para futuros incidentes similares que incluyan métodos para proteger los activos de la empresa lo máximo posible, o al menos los más importantes.
- Finalmente, se contratarán servicios de limpieza especializados independientemente de la gravedad del incidente para limpiar y acondicionar de nuevo el establecimiento así como la reparación de las estructuras afectadas.



Modelo de resolución

El siguiente modelo deberá ser cumplimentado de la siguiente forma por la persona a la que le corresponda en el momento de la resolución de alguno de los incidentes citados anteriormente:

Tipo de incidente
Información detallada
Evidencias
Causas o posibles causas
Resolución del incidente
Correcciones de seguridad
Mejoras propuesta