PLAN DE CONTINGENCIA Y CONTINUIDAD

VENTAJAS DE SU IMPLEMENTACIÓN

Las ventajas de contar con un plan de contingencia y continuidad de las infraestructuras TIC son:

1. **Protección de la información y los sistemas de la organización:** el plan de contingencia y continuidad en infraestructuras TIC establece medidas para proteger la información y los sistemas de la organización ante posibles eventos que paralicen la actividad.
2. **Minimización del impacto de los incidentes y continuidad de las actividades:** estas medidas nos ayudarán a mantener el nivel de producción/servicio en unos límites predefinidos y aceptables.
3. **Cumplimiento normativo:** en algunos casos, la implementación de un plan de contingencia y continuidad en infraestructuras TIC puede ser obligatoria para cumplir con ciertas normativas.
4. **Mejora de la imagen de la organización:** contar con un plan de contingencia y continuidad en infraestructuras TIC puede mejorar la imagen de la organización ante sus clientes y proveedores, ya que demuestra que la organización tiene en cuenta la seguridad de la información y los sistemas.

¿QUÉ INCLUYE?

¿PARA QUÉ SIRVE?

La seguridad al 100% no existe. Las empresas deben estar preparadas protegerse y reaccionar ante posibles incidentes de seguridad que pudieran dañar la capacidad operativa o hacer peligrar la continuidad del negocio.

Un plan de contingencia y continuidad en infraestructuras TIC es un conjunto de medidas que se implementan para garantizar la protección de la información y los sistemas de una organización ante posibles ataques cibernéticos o fallos técnicos.

El objetivo de un plan de contingencia y continuidad en infraestructuras TIC es minimizar el impacto que dichos incidentes puedan tener en la organización y garantizar que la empresa pueda seguir funcionando de manera efectiva.

Es importante recordar que un plan de este tipo debe ser actualizado y probado de forma periódica para asegurar su eficacia y adaptarse a los cambios que puedan surgir en la organización.

Una vez terminadas las etapas anteriores, y recabada la información necesaria, podemos elaborar el Plan de contingencia y continuidad para alcanzar los objetivos de seguridad deseables.

Estos objetivos de seguridad varían según la organización que implante el plan, no obstante, los podemos desglosar en:

Identificación y priorización de activos críticos: identificar qué activos son esenciales para el funcionamiento de la empresa y asegurarse de que estén protegidos en caso de un incidente de seguridad.

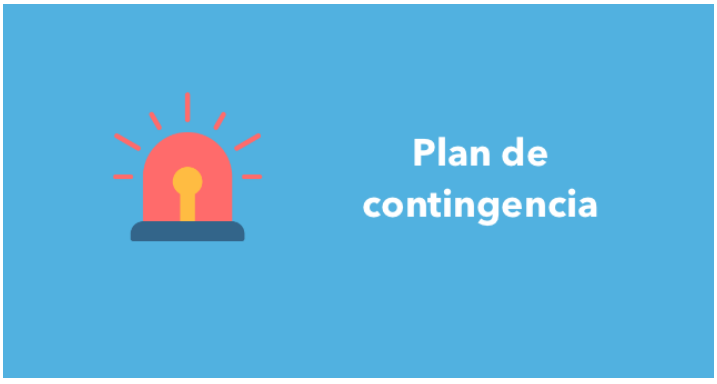
Planes de respuesta: se tienen que establecer planes de respuesta para diferentes tipos de incidentes de seguridad, como ataques de malware, violaciones de datos o interrupciones de servicio.

Estos planes deben incluir medidas para mitigar el impacto y restaurar los servicios de manera rápida y eficiente.

Comunicación: es conveniente tener un plan de comunicación en caso de un incidente de seguridad, para asegurarse de que todos los usuarios estén informados y sepan qué hacer.

Procesos de recuperación: es importante tener planes de recuperación a largo plazo en caso de un incidente grave de seguridad, para asegurarse de que la organización pueda volver a la normalidad lo antes posible.

Pruebas y actualizaciones: se deben realizar pruebas periódicas del plan de contingencia para asegurarse de que está actualizado y efectivo. También se deben realizar actualizaciones periódicas para asegurarse de que está al día con las últimas amenazas y vulnerabilidades de seguridad.



ABF CIBERSEGURIDAD y SISTEMAS

TELÉFONO: 941 10 70 80

info@abfsistemas.es

www.abfsistemas.es