A continuación se citan cinco políticas de seguridad publicadas por INCIBE que ayudan especialmente a las empresas a mantener la confidencialidad, integridad y disponibilidad de la información:

1. Política de clasificación de la información

Esta política ayuda a las empresas a identificar y clasificar la información que deben proteger. Al clasificar la información, las empresas pueden determinar los niveles de confidencialidad, integridad y disponibilidad necesarios para cada tipo de información. Esto les permite implementar las medidas de seguridad adecuadas para proteger cada tipo de información.

2. Política de control de acceso a la información

Esta política ayuda a las empresas a controlar quién tiene acceso a la información. Al establecer controles de acceso, las empresas pueden garantizar que solo las personas autorizadas tengan acceso a la información. Esto ayuda a proteger la confidencialidad de la información.

3. Política de copias de seguridad

Esta política ayuda a las empresas a crear copias de seguridad de la información. Las copias de seguridad protegen la disponibilidad de la información en caso de pérdida, corrupción o destrucción.

4. Política de técnicas criptográficas

Esta política ayuda a las empresas a cifrar la información. El cifrado ayuda a proteger la confidencialidad de la información al hacerla ilegible para los usuarios no autorizados.

5. Política de auditoría

Esta política ayuda a las empresas a auditar la seguridad de sus sistemas de información. Las auditorías ayudan a las empresas a identificar y corregir las vulnerabilidades de seguridad.

Estas políticas ayudan a las empresas a mantener la confidencialidad, integridad y disponibilidad de la información de la siguiente manera:

* Confidencialidad: La clasificación de la información ayuda a las empresas a identificar la información que debe protegerse de accesos no autorizados. Los controles de acceso ayudan a garantizar que solo las personas autorizadas tengan acceso a la información confidencial.
* Integridad: Las copias de seguridad ayudan a proteger la integridad de la información en caso de pérdida, corrupción o destrucción. Las técnicas criptográficas ayudan a proteger la integridad de la información al hacerla ilegible para los usuarios no autorizados.
* Disponibilidad: Las copias de seguridad ayudan a proteger la disponibilidad de la información en caso de pérdida, corrupción o destrucción. Las auditorías ayudan a las empresas a identificar y corregir las vulnerabilidades de seguridad que podrían afectar la disponibilidad de la información.

Además de estas políticas, las empresas también deben implementar medidas de seguridad adicionales para proteger su información. Estas medidas pueden incluir:

* Formación de los empleados en seguridad de la información
* Uso de un sistema de gestión de seguridad de la información (SGSI)
* Implementación de controles de seguridad físicos y lógicos

La implementación de estas políticas y medidas de seguridad ayudará a las empresas a proteger su información de los ciberataques y otros riesgos.

El Instituto Nacional de Ciberseguridad (INCIBE) proporciona una serie de políticas de seguridad que pueden ayudar a las empresas a mantener la Confidencialidad, Integridad y Disponibilidad de la información. Aquí hay cinco de esas políticas y cómo podrían haber ayudado durante un escenario de pandemia:

1. \*\*Política de Acceso y Control de la Información\*\*: Esta política se centra en gestionar quién tiene acceso a la información y en qué condiciones. Durante una pandemia, muchas empresas tuvieron que cambiar rápidamente a modelos de trabajo remoto. Esta política habría ayudado a garantizar que solo las personas autorizadas tuvieran acceso a la información crítica, lo que es esencial para mantener la confidencialidad de los datos.

2. \*\*Política de Copias de Seguridad y Recuperación de Datos\*\*: Una política sólida de copias de seguridad habría permitido a las empresas proteger la integridad de sus datos, ya que los empleados trabajaban desde ubicaciones remotas. En caso de pérdida de datos debido a problemas técnicos o ataques cibernéticos, esta política habría facilitado la recuperación de datos críticos.

3. \*\*Política de Uso Aceptable de Recursos y Tecnologías de la Información\*\*: Durante una pandemia, el uso de dispositivos personales y conexiones no seguras se volvió más común. Esta política habría ayudado a las empresas a establecer directrices claras sobre el uso de recursos y tecnologías de la información, lo que a su vez habría contribuido a mantener la integridad y la disponibilidad de la información.

4. \*\*Política de Gestión de Incidentes de Seguridad de la Información\*\*: En tiempos de crisis, la detección y respuesta a incidentes de seguridad es esencial. Esta política habría proporcionado un marco para la gestión eficiente de incidentes, ayudando a mantener la disponibilidad de la información y reduciendo el impacto de posibles violaciones de seguridad.

5. \*\*Política de Concienciación y Formación en Seguridad de la Información\*\*: En un escenario de pandemia, la capacitación de los empleados en seguridad de la información se vuelve crucial. Esta política habría ayudado a concienciar a los empleados sobre las prácticas seguras al trabajar desde sus hogares, contribuyendo a la confidencialidad e integridad de la información.

La política clave que habría sido fundamental para estar bien preparados durante un escenario de pandemia es la \*\*Política de Continuidad del Negocio y Plan de Contingencia\*\*. Esta política establece un plan estructurado para garantizar la continuidad de las operaciones empresariales en situaciones de crisis, como una pandemia. Ayuda a mantener la disponibilidad de la información y los servicios esenciales al proporcionar un marco para la respuesta a emergencias, la gestión de recursos y la recuperación de operaciones críticas. En una pandemia, esta política sería esencial para garantizar que la empresa pueda seguir funcionando de manera efectiva, independientemente de las circunstancias, manteniendo así la integridad y la disponibilidad de la información.