ACCIÓN D. EJEMPLOS DE BUENAS PRÁCTICAS EN OTRAS UNIVERSIDADES O ADMINISTRACIONES PÚBLICAS Y SU POSIBLE IMPLEMENTACIÓN EN LA UNIVERSIDAD DE ZARAGOZA.

CASO 1

Ya existe un manual de buenas prácticas en el área de informática desarrollado por el INCIBE "Instituto Nacional de Ciberseguridad de España"

Lo primero que debemos hacer es reconocer y clasificar las amenazas que podemos tener, para de esta forma poner los medios necesarios para prevenir y evitar dichas amenazas.

Una vez conocidas las amenazas debemos aplicar e medidas de seguridad básicas. Y aplicación de las medidas organizativas y de cumplimiento legal, además de aplicar medidas para identificar y clasificar los activos.

1. Gestión de los activos:
    - Lo primero es identificarlos (ordenadores personales, teléfonos móviles corporativos, tabletas, portátiles, proyectores, servidores, aplicaciones software, monitores, periféricos, etc.). Es necesario que realicemos y mantengamos actualizado un inventario en el que los activos se encuentren clasificados y gestionados de la manera correcta.
    - Hacer una clasificación que permita aplicar a la misma las medidas de seguridad oportunas. Para la clasificación se pueden considerar, además de su antigüedad y valor estratégico, las tres propiedades: confidencialidad, integridad y disponibilidad.
    - Hacer una adecuada gestión de los soportes para evitar que se revele, modifique, elimine o destruya de forma no autorizada la información almacenada en los mismos.
    - Establecer una gestión de la configuración. Que consiste en diseñar y mantener una Base de Datos de Gestión de configuración que contenga los elementos de configuración necesarios e importantes para proporcionar un servicio (equipos de trabajo, servidores, software de trabajo, redes, documentación, etc.), y la relación existente entre ellos.
2. Seguridad de las operaciones:
    - Son todas las actividades encaminadas a asegurar el correcto funcionamiento del equipamiento donde se realiza el tratamiento de la información, desde su instalación y puesta en marcha, pasando por su actualización y protección ante software malicioso y la realización de copias para evitar la pérdida de datos, hasta la monitorización y el registro de las incidencias.
    - Procedimientos y responsabilidades. Todas las tareas técnicas que realicemos en la organización estén debidamente documentadas. Esto nos permitirá establecer un procedimiento de actuación sobre una determinada tarea, realizándola siempre bajo los mismos criterios. Los procedimientos que elaboremos deben ser diseñados para ser compatibles con futuras y previsibles iniciativas de construcción de nuevos sistemas de información.
    - Instalación de sistemas y aplicaciones. Se debe garantizar que la instalación de los sistemas y aplicaciones: cumplen con los requisitos de seguridad, de la organización. Para ello habría que establecer entornos aislados entre si, en donde se aplicaran todos los parches y actualizaciones necesarios, y se han establecido los acuerdos de nivel de servicio (SLA) y se satisfacen los requisitos de rendimiento y capacidad.
    - Los entornos serían desarrollo, pruebas y producción.
    - Otros aspectos a tener en cuenta son: análisis de las capacidades de los, actualizaciones de seguridad en las aplicaciones, gestión y control de sistemas antivirus, copias de seguridad. gestión de la monitorización

Debemos tener procedimientos para:

- GESTIÓN DE INCIDENTES Y RECUPERACIÓN ANTE DESASTRES.
  - Gestión de incidencias de seguridad
  - Plan de recuperación ante desastres
- CONTROL DE ACCESOS A SISTEMAS Y APLICACIONES
  - Control de accesos a aplicaciones críticas y zonas restringidas
  - Gestión de usuarios y segregación de funciones
  - Gestión segura de las contraseñas

Todo ello implica necesariamente establecer una serie de normas y procedimientos y como no una campaña de información a todos los niveles tanto de desarrolladores como de usuarios.

Así como el establecimiento de canales de comunicación con los usuarios de cara a solucionar los problemas que seguro que le surgirán.

Adjunto como ejemplo el proyecto de la universidad de Granada del 2020 en el que establece un NUEVO MODELO DE ATENCIÓN AL USUARIO. Si bien es algo antiguo, lo incluyo como modelo a seguir para iniciar cualquier proyecto que se quiera iniciar.