Vortech Planes De Contingencia

Descripción del problema:

Como primer pauta del plan de contingencia

será si sucede una pérdida de datos en caso de equivocaciones

Planificación**:**

* Se tendrá que hacer un guardado por cada actualización de los archivos y ser pasado al coordinador para que los guarde.
* En caso de que algún integrante cambie algo del proyecto en GitHub y no avise,se va a ver quién fue en el historial de cambios por si se pierde algún dato
* En caso de que se corrompa un archivo se verá si no hay una versión anterior del mismo sin corromper y sin tantos datos perdidos

Recursos:

Se necesitan estos elementos para el funcionamiento del servidor:

Github

Mysql Workbench 8.0

Visual Studio Code 1.72.1

Descripción del segundo problema:

Como segunda pauta del plan de contingencia

será ante la falla del hardware y/o el software

Planificación**:**

1 - se tendrá que revisar sea cual sea la razón y ver si se puede reparar el equipo para no perder mucho tiempo

2 - si el problema es que el S.O no arranca

se tendrá que utilizar estos recursos

3 - si el daño proviene de la fuente se medirá los voltajes

4 - si el problema es que no funciona algún componente

se hara la revision correspondiente

Recursos:

Github(método de respaldo)

varios Isos de instalación de Windows(Si el S.O no arranca por algún motivo) o en su defecto un usb con la imagen de windows

Un copia de seguridad de windows previo a al incidente

Ejecución:

1. Verificar el estado del hardware para no perder datos

2.

Descripción del tercer problema:

Como tercera pauta del plan de contingencia en esta ocasión será ante el caso de acceso no autorizado al sistema

Planificación:

* Se deberá pedir una medida de autenticación, la cual dejará un registro que será enviado a los administradores los cuales tendrán la opción de bloquear el acceso
* Siempre crear un registro de los cambios realizados si es que logro entrar al sistema y evaluar si hay pérdidas significativas
* En caso de que las pérdidas sean muy grandes tiene que estar la opcion de volver a su estado anterior con un backup

Recursos:

Pendrive con backups

HDD externo

github con backups

Ejecución:

1. al confirmar que la sesión es sospechosa,los administradores bloquearán el acceso

2. en caso de que logrará hacer cambios,si el cambio es menor se puede corregir manualmente,mientras que si el cambio es mayor o total,se cargará el último backup guardado

3.Si se sigue accediendo de forma sospechosa se tendrá que cambiar la contraseña si sigue pasando esto