| Nom i cognoms: Òscar Rodríguez |  |
| --- | --- |
| Data: 12/12/2022 |  |
| Nom de l’activitat/pràctica: ACT430 |  |

**Disposeu d'una aula amb vint-i-cinc ordinadors i un servidor. Aquest servidor treballarà com a servidor d'arxius i disposarà d'un servidor intermediari (proxy), que la resta de màquines utilitzarà per connectar-se a Internet. Les màquines tenen un sistema operatiu Windows i Ubuntu i les aplicacions següents: un paquet d'ofimàtica, un navegador, un paquet d'aplicacions multimèdia i diversos editors de programació.**

**1. Fes un llistat de possibles amenaces, mínim 10. (per exemple: virus/malware, robatoris…)**

* Incendi
* Caiguda de l’electricitat
* Virus informàtic
* Terratrèmol
* Sabotatge
* Falla dels equips informàtics
* Robatori d'equips
* Robatori d’arxius
* Atac informàtic
* Suplantació d’identitat

**2. Per a cada amenaça determina alguna o algunes accions que podem dur a terme dins del pla de recolzament, emergència o recuperació. Utilitzeu la taula següent.**

| **Amenaça** | **Suport** | **Emergència** | **Recuperació** |
| --- | --- | --- | --- |
| Incendi | Fer backups fora de l’aula | Trucar als bombers, tenir extintors a prop i fer el protocol d’evacuació. | Comprovar que estem tots vius, que no s’ha espatllat res i recuperar les dades perdudes. |
| Caiguda de l’electricitat | Tenir instal·lat un sai | Utilitzar el sai | Trucar a la companyía elèctrica perquè torni l’electricitat. |
| Virus informàtic | Tenir instal·lat un antivirus | Utilitzar l’antivirus freqüentment | Comprovar que els equips funcionen correctament. |
| Terratrèmol | Tenir un pla d’evacuació i backups en un altre lloc. | Fer el protocol d’evacuació del recinte on estem. | Comprovar que estem tots vius, que no s’ha espatllat res i recuperar les dades perdudes desde les backups. |
| Sabotatge | Tenir un bon protocol de seguretat i còpies de seguretat | Assignar una persona responsable de la protecció dels equips | Comprovar que els equips funcionen correctament i restaurar les dades perdudes. |
| Falla dels equips informàtics | Netejar els equips informàtics amb freqüència | Comprovar que el hardware funcioni correctament | Realitzar manteniment diari dels equips |
| Robatori d'equips | Fer còpies de seguretat en un disc dur o USB. | Posar una denúncia i comprovar que equips hem perdut | Restaurar les dades perdudes en un altre equip |
| Robatori d’arxius | Fer còpies de seguretat freqüentment | Comprovar que arxius hem perdut | Restaurar les dades perdudes |
| Atac informàtic | Tenir el sistema actualitzat i supervisar les connexions i aplicacions sospitoses | Comprovar que l’equip funciona correctament i que no hem perdut res | Fer l’equip més segur perquè no torni a passar |
| Suplantació d’identitat | Posar contrasenyes més segures | Posar una denúncia | Comprovar que ha fet l’atacant |