

2023-11-23 Comitè Executiu de Seguretat

Data

23-nov-2023

Assistents

- Santi Gallardo
- Ignasi Albors
- Marta Arderiu Prat
- Miquel Estape
- Rubén Cortés
- Ivan Caballero

Ordre del dia

- Aprovació del risc residual de Desa'!. Aprovació del Pla de Tractament de riscos de Desa'!: https://licenciasaoc.sharepoint.com/:f:/s/CiberseguretatAOC/Enjfm77oj1Ms-deZT47ZjABC04QGI_bb6B9CkhuA9Irlw?e=b05lhV
- Aprovació del Pla de Contingència de Desa'!: <https://licenciasaoc.sharepoint.com/:f:/s/CiberseguretatAOC/EuoAnE0s7ZtBqS-4lE8Mt5ABq3zFt0qTqA4rHXBIzrUUKQ?e=tte1h6EI> Pla de Continuitat té 3 documents:
 - BIA: on es justifica el RTO, RPO i MTPD
 - Estratègies de continuïtat: anàlisi de les estratègies de continuïtat per analitzar si s'ajusten al RTO i RPO.

Acta

Punt	Ponent	Títol	Notes																																				
1	Ivan Caballero	Aprovació de l'anàlisi de riscos	<p>S'explica amb detall l'anàlisi de riscos, fent èmfasi en els següents punts:</p> <ul style="list-style-type: none">• Descripció de subdominis de seguretat• Valoració del servei• Càlcul del risc potencial• Càlcul del risc actual• Nivell de risc raonable <p>El Comitè Executiu aprova l'anàlisi de riscos.</p>																																				
2	Ivan Caballero	Aprovació del risc residual de Desa'l	<p>S'explica amb detall el risc actual i amenaces per dominis.</p> <p>Es presenta un pla de tractament dels riscos identificats.</p> <p>El comitè executiu de Seguretat aprova el nivell de risc residual en 3,5.</p> <p>El comitè executiu aprova el pla de tractament del qual s'aplicaran les mesures addicionals per baixar el risc residual a 3.5:</p> <table><tr><th>Prioritat</th><th>ID</th><th>Mesura de seguretat</th><th>Descripció</th><th>Apetit de risc</th></tr><tr><td>7</td><td>1</td><td>[PDS.www] Navegació web</td><td>Inspeccionar i limitar el tràfic web per evitar llocs poc segurs. Inspeccionar els canals xifrats. . Tenir una eina d'inspecció actualitzada. Recuperar el servei de formació i consciència. Control de descàrrega de codi.</td><td>3,6</td></tr><tr><td>5</td><td>2</td><td>[HW. PCD.5.4] Els dispositius mòbils o portàtils s' emmagatzemen en contenidors de seguretat</td><td rowspan="3">Afegeir a la normativa l'ús de dispositius portàtils el control físic dels mateixos.</td><td rowspan="3">3,6</td></tr><tr><td>5</td><td>3</td><td>[HW. PCD.5.3] Els dispositius portàtils es guarden en lloc segur quan no estan en ús</td></tr><tr><td>5</td><td>4</td><td>[HW. PCD.5.1] S' ha establert en quins entorns es pot fer servir l' equip i com</td></tr><tr><td>4</td><td>5</td><td>[IM.1.5] Entrenament</td><td>Fer de forma periòdica, exercicis d'entrenament dels procediments de gestió d'incidents.</td><td>3,6</td></tr><tr><td>4</td><td>6</td><td>[tools. CM.2.3] Correlació d' esdeveniments de seguretat</td><td>Milliores en la detecció d'incidents. Fer correlació dels events de seguretat per detectar incidents</td><td>3,6</td></tr><tr><td>3</td><td>7</td><td>[M.3] Es controla la connexió de dispositius removibles</td><td>Augmentar el control sobre els suports d'informació removibles (discos externs, pendrives, etc.). Requerir autorització prèvia, bloqueig automàtic al inserir, control de la informació transferida.</td><td>3,5</td></tr></table>	Prioritat	ID	Mesura de seguretat	Descripció	Apetit de risc	7	1	[PDS.www] Navegació web	Inspeccionar i limitar el tràfic web per evitar llocs poc segurs. Inspeccionar els canals xifrats. . Tenir una eina d'inspecció actualitzada. Recuperar el servei de formació i consciència. Control de descàrrega de codi.	3,6	5	2	[HW. PCD.5.4] Els dispositius mòbils o portàtils s' emmagatzemen en contenidors de seguretat	Afegeir a la normativa l'ús de dispositius portàtils el control físic dels mateixos.	3,6	5	3	[HW. PCD.5.3] Els dispositius portàtils es guarden en lloc segur quan no estan en ús	5	4	[HW. PCD.5.1] S' ha establert en quins entorns es pot fer servir l' equip i com	4	5	[IM.1.5] Entrenament	Fer de forma periòdica, exercicis d'entrenament dels procediments de gestió d'incidents.	3,6	4	6	[tools. CM.2.3] Correlació d' esdeveniments de seguretat	Milliores en la detecció d'incidents. Fer correlació dels events de seguretat per detectar incidents	3,6	3	7	[M.3] Es controla la connexió de dispositius removibles	Augmentar el control sobre els suports d'informació removibles (discos externs, pendrives, etc.). Requerir autorització prèvia, bloqueig automàtic al inserir, control de la informació transferida.	3,5
Prioritat	ID	Mesura de seguretat	Descripció	Apetit de risc																																			
7	1	[PDS.www] Navegació web	Inspeccionar i limitar el tràfic web per evitar llocs poc segurs. Inspeccionar els canals xifrats. . Tenir una eina d'inspecció actualitzada. Recuperar el servei de formació i consciència. Control de descàrrega de codi.	3,6																																			
5	2	[HW. PCD.5.4] Els dispositius mòbils o portàtils s' emmagatzemen en contenidors de seguretat	Afegeir a la normativa l'ús de dispositius portàtils el control físic dels mateixos.	3,6																																			
5	3	[HW. PCD.5.3] Els dispositius portàtils es guarden en lloc segur quan no estan en ús																																					
5	4	[HW. PCD.5.1] S' ha establert en quins entorns es pot fer servir l' equip i com																																					
4	5	[IM.1.5] Entrenament	Fer de forma periòdica, exercicis d'entrenament dels procediments de gestió d'incidents.	3,6																																			
4	6	[tools. CM.2.3] Correlació d' esdeveniments de seguretat	Milliores en la detecció d'incidents. Fer correlació dels events de seguretat per detectar incidents	3,6																																			
3	7	[M.3] Es controla la connexió de dispositius removibles	Augmentar el control sobre els suports d'informació removibles (discos externs, pendrives, etc.). Requerir autorització prèvia, bloqueig automàtic al inserir, control de la informació transferida.	3,5																																			

3	Ivan Caballero	Aprovació del pla de contingència de negoci (PCN)	<p>Es presenten els documents del Pla de Contingència.</p> <p>BIA.</p> <p>El Comitè Executiu no està d'acord amb el nivell MTPD a 24h per ser massa restrictiu i decideix fixar aquest valor en 48h.</p> <p>El Comitè Operatiu aprova la resta del document.</p> <p>Estratègies de continuïtat.</p> <p>El Comitè Operatiu deixa constància de la seva preocupació perquè una restauració total de les dades no es podria fer dins del temps de RTO. Segons s'ha extret de les proves de restauració de backup, una restauració completa de les dades trigaria 13h.</p> <p>El Comitè Operatiu aprova el document d'estratègies de continuïtat, però fa l'encàrrec al Comitè Operatiu d'estudiar nous mecanismes de restauració on no calgui restaurar la totalitat de les dades en el procediment de Disaster Recovery.</p>
---	-------------------	---	--