RECOMENDACIONES GENERALES QUE CONTRIBUYEN A ELEVAR EL NIVEL DE PROTECCIÓN Y RESILIENCIA DE LAS EMPRESAS VASCAS FRENTE A LOS CIBERATAQUES

1. Configuración segura de dispositivos

Las **configuraciones por defecto** no son siempre las más idóneas desde una perspectiva de ciberseguridad.

2. Control y configuración segura de aplicaciones

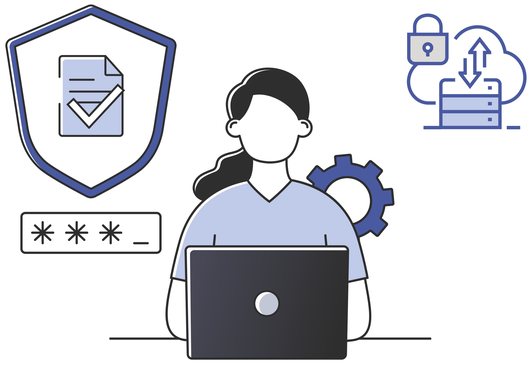
Limitar el número de aplicaciones, instalando y utilizando únicamente aquellas destinadas a la operativa habitual de trabajo. Así mismo, se recomienda **limitar los permisos** de los usuarios aplicando la ley del mínimo privilegio, de modo que únicamente puedan realizar aquellas tareas necesarias para su desempeño profesional diario. Se recomienda que los usuarios finales no tengan rol de administrador.

3. Protección frente a programas maliciosos

Utilizar y mantener **actualizada una solución antivirus con protección ransomware**, siendo muy recomendable el añadir solución EDR, y realizar escaneos periódicos. Así mismo, se recomienda **apagar aquellos dispositivos que no estén en uso** para que en el caso del compromiso del sistema no se vean afectados.

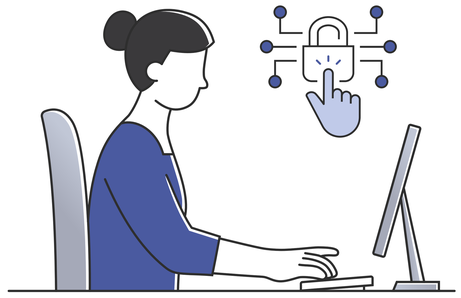
4. Protección de las conexiones

En caso de requerir acceso remoto, habilitarlo mediante **VPN** llevando un control y teniendo un inventario detallado de todos los accesos autorizados. Así mismo, **limitar el perímetro,** bloqueando por defecto accesos provenientes de localizaciones no habituales como por ejemplo países desde los que no deberían realizar conexiones a nuestra infraestructura. De igual modo, **limitar las conexiones salientes** a sitios incluidos en listas de reputación catalogados como maliciosos.



5. Copias de seguridad

Establecer y mantener una **política de copias de seguridad** siguiendo la directriz 3, 2, 1: 3 copias de seguridad en 2 soportes distintos y almacenar 1 de ellas aislada completamente fuera de la red. Realizar dichas copias con una **periodicidad que permita recuperar la actividad en un plazo óptimo** en caso de ser necesaria su utilización. Así mismo, se recomienda **validar el funcionamiento** de dichas copias y del proceso de restauración.



6. Actualizaciones de seguridad

Establecer una política de actualizaciones para poder aplicarlas en el menor tiempo posible, evitando de esta forma la potencial explotación de vulnerabilidades conocidas. Hacer hincapié en **priorizar la aplicación de parches** sobre entornos expuestos y especialmente en el caso de vulnerabilidades altas y críticas.

7. Control de accesos

Activar la **autenticación mediante múltiples factores** siempre que sea posible, especialmente en aquellos casos en los que impliquen accesos externos, accesos a cuentas con privilegios, etc. Así mismo, **establecer una política de cambio de contraseñas** que recoja su modificación periódica, forzando el reseteo en el caso de que no se hayan modificado en un plazo de 6 meses. Esto es especialmente importante en el caso de usuarios con rol de administración.

8. Concienciación

Recordar a los empleados la necesidad de **extremar las precauciones** durante el manejo de correos electrónicos y adjuntos.

9. Alerta temprana

En caso de identificar actividad maliciosa, **reportar inmediatamente** a la persona responsable de seguridad / sistemas para que pueda tomar las medidas oportunas para mitigar el impacto, aislarse del resto de organismos y notificar a través de los canales establecidos.

SI IDENTIFICAS UNA CAMPAÑA ACTIVA DE MALWARE O PHISHING PUEDES AVISARNOS:

Llamando al 900 104 891

Enviando un email a incidencias@bcsc.eus