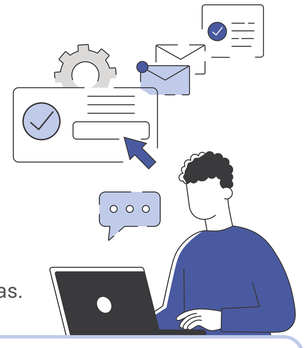
MEDIDAS TÉCNICAS QUE CONTRIBUYEN A ELEVAR EL NIVEL DE PROTECCIÓN Y RESILIENCIA DE LAS EMPRESAS VASCAS

NAVEGACIÓN

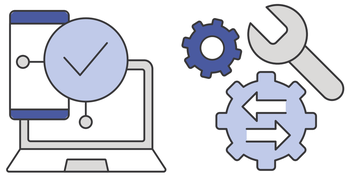


- Recalcar la importancia de navegar de **forma segura** únicamente a sitios necesarios por el ámbito laboral.
- Extremar las **precauciones** al acceder a sitios desconocidos o a través de enlaces.
- Revisar que el **proxy** está correctamente configurado para bloquear el acceso a sitios maliciosos.
- Configurar los **firewalls** para que bloqueen páginas web catalogadas como maliciosas.

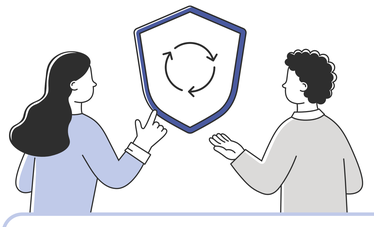
CORREO

- Implementar y revisar la **correcta configuración** de los registros SPF, DKIM, DMARC y DNSSEC.
- Revisar la configuración del correo electrónico y **comprobar los filtros** de protección (detección de malware, phishing, etc.).
- Valorar **bloquear ciertas tipologías de ficheros** potencialmente dañinas, como por ejemplo aquellos que permiten incrustar macros o al menos bloquear la ejecución de macros si es posible. Así mismo, limitar la ejecución de herramientas de línea de comandos como powershell o wmic.

CONFIGURACIÓN SEGURA DE DISPOSITIVOS



- Tener en cuenta **buenas prácticas** de ciberseguridad.
- Establecer y seguir un proceso de **gestión de vulnerabilidades**.



ACTUALIZACIONES DE SEGURIDAD

- Mantener los **sistemas actualizados**.
- Verificar que las actualizaciones proceden de **fuentes confiables**.
- Hacerlo de **forma escalonada** para minimizar el impacto de errores o actualizaciones maliciosas.

MONITORIZACIÓN

- **Activar la recogida de eventos / logs de seguridad sistema**, (incluyendo herramientas de línea de comandos), endpoint, firewalls, proxy, etc.) y revisarlos en busca de actividad anómala.
- **Monitorizar los eventos del sistema** para identificar actividad sospechosa asociada a cuentas privilegiadas, como pueden ser intentos fallidos de autenticación, acceso a unidades de almacenamiento compartido, o inicios de sesión en sistemas inusuales o creación de cuentas nuevas.
- **Revisar los flujos de red** en busca de signos de actividad anómala.
- Asegurarse de que los **dispositivos de red registren y auditen** todos los cambios de configuración.

PROTECCIÓN DE LAS CONEXIONES:

- Utilizar una **adecuada segmentación de la red**.
- Asegurarse de que las conexiones entre sistemas tienen en cuenta el **principio de mínimo privilegio**.

- Verificar que están **documentadas y autorizadas**.
- Utilizar **redes o VLAN** específicas para el acceso a la gestión de los sistemas más críticos, como los de red y almacenamiento.
- **Monitorizar la comunicación de los sistemas** que puedan emplearse para "moverse lateralmente" entre los sistemas de la infraestructura, y verificar que se encuentran correctamente fortificados.
- Valorar **bloquear el tráfico de TOR**.

CONTROL DE ACCESO

- Utilizar un **segundo factor** de autenticación (o múltiples).
- Asegurarse de que los usuarios de dominio estén **asignados a un subconjunto específico del personal** de la empresa y no puedan acceder o autenticarse directamente en sistemas críticos.
- Documentar y configurar según el concepto de **mínimo privilegio** los permisos asignados a los usuarios.
- Disponer de **capacidad de monitorización** de las acciones que realizan los usuarios.
- Revisar de forma periódica la **asignación de permisos**, restringiendo aquellos que no sean necesarios.

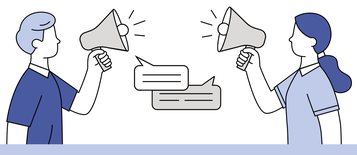
CONTINUIDAD DE NEGOCIO

- Establecer un **comité de crisis** identificando personas, roles e información de contacto para que sean notificadas en caso de incidente.
- Elaborar **planes de respuesta** a incidentes.
- Elaborar **planes de recuperación** frente a desastres.

- Elaborar **planes de continuidad** de negocio.
- Realizar **ejercicios de simulación** para validar dichos planes.
- **Identificar a los proveedores críticos y fijar cláusulas** en las que se establezca su obligatoriedad de notificar en plazos mínimos si sufren un incidente de ciberseguridad.

ALERTA TEMPRANA

- Seguir **avisos y alertas** de ciberseguridad sobre campañas de malware o vulnerabilidades.



En caso de requerir servicios especializados de ciberseguridad se puede consultar el catálogo de proveedores en **https://www.basquecybersecurity.eus/es/buscador-empresas**

En caso de identificar una campaña activa de malware o phishing es posible reportárnosla a **incidencias@bcsc.eus** para mitigarla y evitar así su propagación.