CONTROL: 8.20 SEGURIDAD DE LOS SERVICIOS DE RED

1. Propósito

El control 8.20 requiere que se aseguren los servicios de red subyacentes y de soporte (como DNS, NTP, DHCP, SMTP) contra el acceso no autorizado, la modificación, el fallo o la denegación de servicio. La falta de seguridad en estos servicios podría comprometer la **disponibilidad** (ej. fallo del DNS que impide la conexión App-Servidor) y la **integridad** (ej. manipulación de la hora NTP que afecta el registro de evidencia).

Para "Alerta Mujer", la seguridad de estos servicios es crítica para garantizar que la aplicación pueda **conectar de manera confiable** y que el **registro de eventos y alertas sea preciso** (RF9.1, 8.17).

2. Procedimiento de Aplicación del Control 8.20

La implementación de este control se centrará en dos servicios clave identificados: **DNS** (Sistema de Nombres de Dominio) y **NTP** (Protocolo de Tiempo de Red).

2.1. Seguridad del Servicio DNS

El DNS traduce el nombre de dominio del servidor de "Alerta Mujer" a una dirección IP. Su seguridad es vital para prevenir el secuestro de sesiones (*phishing*).

- **Fuentes Confiables:** Se debe utilizar un **servicio DNS gestionado y robusto** (generalmente ofrecido por el proveedor de *cloud* o *hosting*) que ofrezca protección contra ataques de Denegación de Servicio Distribuido (DDoS).
- **Zona de Hosteo:** La administración de la zona DNS (donde se configuran los registros) debe estar protegida mediante **Autenticación Multifactor (MFA)** para cualquier cambio.
- **Zonificación:** Se implementará DNS dividido (*Split-Horizon DNS*) si es necesario, asegurando que los registros internos (ej. para la Red de Administración) no sean visibles al público (Red de Producción).
- **Monitorización:** Se configurará el monitoreo para **detectar cambios no autorizados** en los registros DNS críticos de la aplicación (Control 8.16 faltante).

2.2. Seguridad del Servicio NTP (Sincronización de Reloj)

La hora correcta es fundamental para el registro de alertas y evidencias (8.17).

- **Fuentes Confiables:** Los servidores de aplicación y base de datos deben configurarse para sincronizar la hora únicamente con **servidores NTP internos o de alta reputación** (ej. NTP *pool* con protección o servicio del proveedor de *cloud*).
- **Restricción de Acceso:** El acceso al servicio NTP en los servidores (puerto UDP 123) debe **restringirse vía *firewall*** únicamente a las IPs de los servidores de aplicación y BD, y prohibirse el acceso externo (Control 8.19).
- **Monitorización de Desviación:** Se implementarán herramientas para monitorear la **desviación de tiempo** (*time drift*) de los servidores y generar alertas si supera un umbral definido, garantizando la precisión del registro de tiempo.

2.3. Configuración Segura (*Hardening*)

Cualquier servidor o dispositivo que ofrezca un servicio de red (ej. *firewall*, *router*, balanceador de carga) debe ser configurado de forma segura.

- **Deshabilitar Servicios Innecesarios:** Todos los servicios de red que no sean esenciales para la operación (ej. SSH sin uso, FTP, *Legacy Protocols*) deben ser **deshabilitados o eliminados**.
- **Actualizaciones:** Se debe incluir la gestión de parches de seguridad para los componentes de red en el proceso formal de Gestión de Vulnerabilidades (Control 8.8 faltante).