Bases técnicas de Seguridad Informática para las dependencias y entidades de la Administración Pública Federal

Coordinación de Estrategia Digital Nacional

12 de marzo de 2020

1. Bases técnicas de seguridad informática

Las siguientes son recomendaciones mínimas de seguridad informática, cuya formulación considera un enfoque de seguridad en profundidad, características de seguridad de la información, así como acciones de prevención, detección y respuesta ante incidentes.

1.1. Medidas de prevención de incidentes

1. Realizar un inventario de todos los activos de información donde se identifiquen los datos, la información y los sistemas, sensibles o críticos para la institución. Se debe proteger y restringir el acceso a dicho inventario solo al personal autorizado.

2. Elaborar un plan de contingencia que defina las acciones, procedimientos, responsabilidades y contactos para minimizar el impacto de una interrupción de las funciones críticas de la institución.

3. Establecer un procedimiento para la gestión de incidentes de seguridad que debe contemplar acciones inmediatas, los actores que intervienen y las responsabilidades de evaluación e información sobre el incidente.

4. Establecer controles de seguridad física para el centro de procesamiento de datos y la bóveda de respaldos.

5. Establecer como política de red de perímetro en *firewalls* el cierre de todos los puertos por defecto y la apertura los servicios únicamente cuando sean solicitados y autorizados.

6. Establecer un monitoreo y control de los accesos remotos. Implementar *firewalls* para el acceso exclusivo de las aplicaciones y servicios necesarios.

7. Realizar copias de respaldo de seguridad de los dispositivos de red, servidores físicos, servidores virtuales, servicios, accesos de aplicaciones, bases de datos, entre otra información sensible.

    - Establecer procesos y/o procedimientos de respaldo incluyendo la periodicidad.
    - Realizar sumas de verificación de la información respaldada.
    - Mantener un registro de los respaldos de información y su suma de verificación.
    - Realizar pruebas de restauración de las copias de respaldo.
    - Determinar tiempos de retención de las copias de respaldo.
    - Almacenar las copias de respaldo en diferentes ubicaciones y medios digitales.
    - Nunca almacenar los respaldos de seguridad en la misma infraestructura.

8. Segmentar las redes separando los servidores de los usuarios no autorizados. Separar las distintas zonas con un *firewall*, de manera que los sistemas y servicios solo sean accesibles cuando se cuente con la autorización.

9. Implementar herramientas de análisis de tráfico de red para prevenir y detectar intrusiones o anomalías.

10. Deshabilitar por defecto la función *Wake on LAN* para evitar que los equipos se enciendan remotamente.

11. Implementar reglas de filtrados de contenido mediante *proxys* en la red interna.

12. Establecer listas blancas de acceso a páginas web.

13. Realizar un fortalecimiento de los servidores (*hardening*), implementar *firewall* de *host*, restringir todos los accesos innecesarios, abrir solo los puertos requeridos.

14. Hacer uso de herramientas de bloqueo y prevención, como *anti-ransom*, filtros anti-*spam*, anti-*malware*, antivirus y bloqueadores *JavaScript*.

15. Establecer políticas de seguridad en los servidores para impedir la ejecución de programas utilizados por el *malware*.

16. Priorizar el uso de servidores virtualizados que permitan escalabilidad y disponibilidad.

17. Utilizar comunicaciones cifradas entre servidores y entre aplicaciones.

18. Implementar protocolos de autenticación segura para identificación y autorización de usuarios en las redes, con asignación de roles, privilegios y permisos.

19. Actualizar a las últimas versiones con los parches de seguridad mas recientes de los sistemas operativos, controladores de *software* (*drivers*) y aplicaciones.

20. Utilizar servidores de correo institucional. Evitar utilizar servidores de correo comerciales. Configurar el SMTP para que únicamente reciba correo de dominios válidos. Utilizar cuentas de usuario autenticadas para prevenir y controlar suplantación de correo. En lo posible hacer uso de las aplicaciones anti-*spam*.

21. Utilizar sistemas operativos que reciban actualizaciones continuas y permitan la revisión de su código fuente. Priorizar la migración y el uso de sistemas operativos GNU/Linux y *Software* Libre.

22. Restringir el acceso a servicios web públicos, mediante filtros geográficos de acceso el contenido.

23. Utilizar contraseñas únicas por cada servidor o software que se administre.

24. Implementar bloqueadores *JavaScript* en el navegador, mostrar extensiones de archivos, utilizar herramientas a Anti-*Ransom* a nivel de *host* de usuarios.

25. Capacitar a los usuarios en identificación de amenazas, buenas prácticas de seguridad informática y respuesta ante incidentes.

26. Definir una política de contraseñas utilizando una serie de palabras inconexas en lugar de una única palabra cuando sea posible. Utilizar contraseñas con números y caracteres especiales. Revisar la fortaleza de seguridad de las contraseñas.

27. Priorizar el uso de distintos factores de autenticación en sistemas y software desarrollados.

28. Cambiar contraseñas por defecto u otorgadas por el fabricante.

29. Implementar software de bloqueo y filtrado de los puertos usb de los equipos de los de usuarios.

1.2. Mecanismos para la detección y correlación de eventos

1. Rastrear y supervisar los accesos a los recursos de red, servidores, servicios e información.

2. Implementar sistemas de monitoreo que alerten sobre comportamientos anómalos en las redes de datos.

3. Establecer monitoreo de los recursos de los servidores y bases de datos.

4. Implementar sistemas de detección y prevención de intrusos en los equipos de cada usuario.

5. Implementar sistemas de detección y prevención de intrusos en la red.

6. Realizar análisis y correlación de eventos para identificar posibles amenazas.

1.3. Acciones de respuesta ante impacto de un incidente

1. Mantener un registro detallado de todos los incidentes de seguridad informática.

2. Realizar la recolección de evidencias conservando su integridad.

3. Observar una cadena de custodia que sea íntegra y verificable para preservar las evidencias forenses.

4. Identificar el tipo de incidente, notificar, clasificar y priorizar de acuerdo al plan de contingencia.

5. No establecer contacto ni entrar en negociación con los autores de un ataque o secuestro de información (*ransomware*).

6. Cuando sea posible se debe hacer una copia exacta de los discos duros de los equipos infectados con su respectiva suma de verificación

7. Si no es posible realizar la copia del disco entero, se debe realizar un respaldo de los artefactos forenses de acuerdo al sistema operativo, con su respectiva suma de verificación.

8. Equipo de respuesta de incidentes entregará los artefactos que ayude a la investigación forense posterior.

9. Recuperar los archivos cifrados si fuera posible.

10. Restaurar los equipos para continuar con la actividad, reinstalando el equipo con el *software* original y restaurando la información de la última copia de seguridad realizada.