Escuela Politécnica Nacional

Dirección de Gestión de la Información y Procesos

CENTRO DE RESPUESTA A INCIDENTES DE SEGURIDAD (CSIRT-EPN)

EPN-DGIP-CSIRT-05-DI

REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA NUEVOS SERVICIOS, SOLUCIONES O APLICACIONES DE TI DE LA EPN

Levantamiento requerimientos de seguridad	Centro de Respuesta a Incidentes de Seguridad CSIRT-EPN	Ing. Javier Erazo	
		Ing. David Quinchaguano	
		Daniela Córdova	
Revisión y aprobación de requerimientos de seguridad	Dirección de Gestión de la Información y Procesos	Ing. Mónica Játiva	
		Ing. Geovanna Saltos	
		Ing. Juan Carlos Proaño	
		Ing. Pablo Ortiz	

Autorizado	Director DGIP	Ing. Roberto Andrade, MSc.	

EPN-DGIP-CSIRT-05-DI

HOJA DEL ESTADO DEL DOCUMENTO

TITULO DEL DOCUMENTO: REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA NUEVOS SERVICIOS, SOLUCIONES O APLICACIONES DE TI DE LA EPN.

ESTADO DEL DOCUMENTO: Para aprobación

1. QUIEN EDITA	2. QUIEN REVISA	3. FECHA	4. RAZONES DE CAMBIO/QUIEN CAMBIA
Javier Erazo	Líderes de área DGIP	4/sept/2017	Creación documento
Daniela Córdova	Líderes de área DGIP	30/10/2017	Cambios al documento

1. OBJETIVO

Determinar los lineamientos de seguridad que deben cumplir todos los servicios, soluciones y aplicaciones que se vayan a implementar o a ser adquiridos por la Escuela Politécnica Nacional que involucren el uso de recursos de TI.

La implementación de un nuevo servicio, solución o el desarrollo de una nueva aplicación, involucra componentes de hardware y software. Los **Requerimientos de Seguridad de la Información - RSI**, buscan que la Escuela Politécnica Nacional – EPN cuente con servicios, soluciones o aplicaciones seguras, menos vulnerables, mitigando de esta manera el riesgo de que la información de la Institución sea comprometida o vulnerada, tras la ejecución de un ataque informático y explotación de vulnerabilidades presentes en servicios o aplicaciones inseguras.

Los Requerimientos de Seguridad de la Información aquí expuestos, están sujetos a actualizaciones periódicas en función de la identificación de nuevos riesgos de seguridad y de nuevas normativas de seguridad internas y/o externas.

2. ALCANCE

Los Requerimientos de Seguridad de la Información son de cumplimiento obligatorio y deben ser incluidos desde la fase de análisis de los desarrollos in house, en la fase precontractual, desde la formulación de los términos de referencia (TDR), previo la contratación, desarrollo y/o adquisición de un nuevo servicio, solución o aplicación o cualquier componente de hardware o de software que sea desarrollado y/o adquirido por la Institución.

3. RESPONSABILIDAD Y AUTORIDAD

El responsable para definir, actualizar y vigilar la implementación de los requerimientos de seguridad en un nuevo servicio, solución o el desarrollo de una nueva aplicación en la EPN es:

Centro de Respuesta a Incidentes de Seguridad CSIRT-EPN

Los responsables de revisar y aprobar estos lineamientos son:

Líderes de área de la DGIP

El responsable de autorizar la implementación de estos lineamientos es:

Director de la Dgip

La autoridad para hacer cumplir estos lineamientos son:

Autoridades de las Unidades Académicas y Administrativas de la EPN.

Los responsables de cumplir estos lineamientos son:

Miembros de la Comunidad Politécnica, que gestionen la contratación, desarrollo y/o adquisición de un nuevo servicio, solución o aplicación o cualquier componente de hardware o de software que sea desarrollado y/o adquirido por la Institución.

4. INCLUSIÓN DE REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN EN PROCESOS DE CONTRATACIÓN DE LA EPN

Previo la contratación, desarrollo y/o adquisición de un nuevo servicio, solución o aplicación, o cualquier componente de hardware o de software, se debe insertar según corresponda y aplique dependiendo del

proyecto, los ítems de la sección que se detalla a continuación como Requerimientos de Seguridad de la Información que son de cumplimiento obligatorio.

CUMPLIMIENTO DE TÉRMINOS DE REFERENCIA Y ESPECIFICACIONES TÉCNICAS			
ÍTEM	DESCRIPCIÓN	CALIFICACIÓN	
1	ESPECIFICACIONES GENERALES SERVICIO/SOLUCIÓN/APLICACIÓN	Cumplimiento	Condiciones de Cumplimiento
Requerimientos de Seguridad	El oferente deberá cumplir con las políticas, normativas, procedimientos, procesos, estándares y lineamientos de seguridad de la información vigente en la EPN, que sean aplicables a la plataforma a ser contratada con las debidas justificaciones técnicas.	Obligatorio	
	El oferente deberá garantizar que la solución ofertada no tenga vulnerabilidades de seguridad, para lo cual se requiere que el Centro de Respuesta a Incidentes de Seguridad CSIRT-EPN, elabore un informe favorable, y en el caso de ser detectadas el oferente deberá gestionar su remediación. La EPN ejecutará la revisión de vulnerabilidades previo el paso a producción para verificar el presente requerimiento.	Obligatorio	
	El oferente deberá garantizar que la solución ofertada provea las funcionalidades de gestión de usuarios como: a. Número limitado de intentos fallidos.	Obligatorio	
	b. Tiempo de inactividad del usuario tras el cual se cerrará la sesión.	Obligatorio	
	c. Máximo de sesiones concurrentes por usuario.	Obligatorio	
	d. Almacenamiento de contraseñas en forma cifrada.	Obligatorio	
	La solución deberá generar registros de auditoria, tales como accesos fallidos o exitosos, modificaciones o eliminaciones de los registros por parte de los usuarios. Deberá contener como mínimo: Qué, quién, cuándo, cómo y dónde.	Obligatorio	
	El oferente debe garantizar que la solución ha sido desarrollada usando prácticas de desarrollo seguro de software.	Obligatorio	

Dependiendo del proyecto la DGIP verifica durante el Proceso de Gestión de Cambios y previo el paso a producción, del nuevo servicio, solución o aplicación, o cualquier componente de hardware o de software adquirido o desarrollado, la inclusión de los Requerimientos de Seguridad, mediante el proceso determinado para el efecto.

5. TIPOS DE REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Los Requerimientos de Seguridad de la Información se han dividido en:

- Requerimientos de Seguridad de la Información para componentes de Hardware y software.
  - Servidores
  - Equipos de redes, comunicaciones y seguridad informática
- Requerimientos de Seguridad de la Información para Aplicaciones.

5.1. REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA COMPONENTES DE HARDWARE Y SOFTWARE

SERVIDORES: Incluye sistema operativo, utilitarios, base de datos y software adicional que puede ser instalado en servidores que soportarán el servicio, solución o aplicación a implementar.

Si una aplicación es propietaria (no requiere desarrollo), pero requiere de un componente de hardware (por ejemplo, un servidor) y de un componente de software (por ejemplo, un utilitario o una base de datos) para su implementación; los RSI que deben ser incluidos son:

1. Procedimientos de Hardening[1] en el servidor para sistema operativo y software adicional aplicados.
2. El sistema operativo y software adicional permite el cambio de contraseñas en un período de tiempo definido para los usuarios creados.
3. Las cuentas creadas por defecto en el sistema operativo y software adicional están deshabilitadas.
4. Roles para uso de los componentes del servicio, solución o aplicación asignados de acuerdo a las políticas de seguridad de la información.
5. Para servicios cuenta genérica creada, asignada y registrada para servicio.
6. Cuenta adicional para administración creada, asignada y registrada.
7. Clave de administrador principal del sistema bajo custodia de Seguridad de la Información.
8. Acceso directo con usuarios administradores deshabilitado.
9. Permite la configuración de alerta automática para cambio de contraseñas en un período de tiempo definido antes de su expiración.
10. Permite el uso de autenticación centralizada (Directorio Activo).
11. Previo a la publicación de información, la autenticación debe ser exitosa.
12. En caso de que no permita el uso de autenticación centralizada, permite la configuración de Políticas de Seguridad de la Información - PSI.
13. La Unidad requirente fue notificada del proceso de entrega y reseteo de credenciales
14. Permite que la construcción de claves se apegue al estándar definido en la Institución.
15. El sistema operativo restringe el uso de las últimas cinco contraseñas utilizadas.
16. El sistema operativo permite el bloqueo de acceso al tercer intento fallido de sesión.
17. El sistema operativo permite el reseteo de contraseña luego del primer inicio de sesión.
18. El sistema operativo permite el cifrado[2] de contraseñas.
19. El sistema operativo cuenta con el log de monitoreo para autenticación de usuarios activado.
20. No existen cuentas huérfanas en el sistema operativo y software adicional creadas.
21. La Unidad requirente fue notificada de que el acceso de usuarios externos es autorizado por Seguridades de la Información.
22. El sistema operativo y software adicional cuenta con las últimas actualizaciones de seguridad aplicadas.
23. El servidor cuenta con el Antivirus instalado y actualizado.
24. El servidor está registrado en el inventario actualizado de equipos y dispositivos de la Institución.
25. El sistema operativo del servidor está registrado en el inventario actualizado de sistemas operativos de la Institución.
26. El software adicional del servidor está registrado en el inventario actualizado de aplicativos usados en equipos de tecnología
27. Las licencias de sistema operativo y software adicional instalado en el servidor están registradas en el inventario actualizado de licenciamiento de la Institución.
28. El Catálogo de servicios fue actualizado.
29. El sistema operativo, utilitarios, base de datos y software adicional obtuvo resultados positivos, es decir que no presenta vulnerabilidades de criticidad alta, luego de ser sometido a un análisis de vulnerabilidades.

[1] Hardening, (palabra en ingles que significa endurecimiento), en seguridad informática es una estrategia defensiva que protege contra los ataques removiendo servicios vulnerables e innecesarios, cerrando "brechas" de seguridad y asegurando los controles de acceso.

[2] Cifrado: procedimiento que utiliza un [[algoritmo con cierta clave (clave de cifrado) transforma un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo.

EQUIPOS DE REDES, COMUNICACIONES Y SEGURIDAD INFORMÁTICA: Incluye Router, switch, AP, filtrado Web, firewall, Siem, Dam, Analizador de vulnerabilidades, Analizador de código, etc.

Los Requerimientos de Seguridad de la Información cuando la puesta en producción de un nuevo servicio involucra la adquisición de equipos de redes, comunicaciones y seguridad informática son:

1. Procedimientos de Hardening de equipos aplicados.
2. Los equipos permiten el cambio de contraseñas en un período de tiempo definido para los usuarios creados
3. Las cuentas creadas por defecto en los equipos están deshabilitadas.
4. Roles para uso de los componentes del servicio, solución o aplicación asignados de acuerdo a las políticas de seguridad de la información.
5. Para servicios cuenta genérica creada, asignada y registrada para servicio.
6. Cuenta adicional para la administración creada, asignada y registrada.
7. Clave de administrador principal del sistema bajo custodia de Seguridad de la Información.
8. Acceso directo con usuarios administradores deshabilitado.
9. Permite la configuración de alerta automática para cambio de contraseñas en un período de tiempo definido antes de su expiración.
10. Permite el uso de autenticación centralizada (Directorio Activo).
11. Previo a la publicación de información, la autenticación debe ser exitosa.
12. En los equipos el SNMP (v3 y string community) debe estar configurado.
13. La Unidad requirente fue notificada del proceso de entrega y reseteo de credenciales
14. Permite que la construcción de claves se apegue al estándar definido en la Institución.
15. Los equipos restringen el uso de las últimas cinco contraseñas utilizadas.
16. Los equipos permiten el bloqueo de acceso al tercer intento fallido de sesión.
17. Los equipos permiten el reseteo de contraseña luego del primer inicio de sesión.
18. Los equipos permiten el cifrado de contraseñas.
19. Los equipos cuentan con el log de monitoreo para autenticación de usuarios activado.
20. No existen cuentas huérfanas creadas en los equipos.
21. La Unidad requirente fue notificada de que el acceso de usuarios externos es autorizado por Seguridades de la Información.
22. Los equipos cuentan con las últimas actualizaciones de seguridad aplicadas.
23. Los equipos están registrados en el inventario actualizado de equipos y dispositivos de la institución.
24. El sistema operativo de los equipos está registrado en el inventario actualizado de sistemas operativos de la Institución.
25. Los equipos están registrados en el inventario actualizado de aplicativos usados en equipos de tecnología.
26. Las licencias de los equipos están registradas en el inventario actualizado de licenciamiento de la Institución.
27. El Catálogo de servicios fue actualizado.
30. El equipo de redes, comunicaciones o seguridad informática obtuvo resultados positivos, es decir que no presenta vulnerabilidades de criticidad alta, luego de ser sometido a un análisis de vulnerabilidades.

5.2. REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA APLICACIONES

DESARROLLO DE APLICACIONES: Incluye el desarrollo de aplicaciones internas y externas (para consumo de los miembros de la comunidad politécnica y de la ciudadanía en general).

Si el nuevo servicio involucra el desarrollo de una nueva aplicación que pasará por las fases de desarrollo, preproducción y producción, se deberá tomar en cuenta los siguientes requerimientos de seguridad de la información:

1. Requerimientos de seguridad de la información para sus componentes de Hardware y Software aplicados.
2. La aplicación permite el cambio de contraseñas en un período de tiempo definido para los usuarios creados.
3. Las cuentas creadas por defecto en la aplicación están deshabilitadas.
4. Roles para uso de la aplicación asignados de acuerdo a las políticas de seguridad de la información.
5. Cuenta adicional para administración creada, asignada y registrada.
6. Clave de administrador principal de la aplicación bajo custodia de Seguridad de la Información.
7. Acceso directo con usuarios administradores deshabilitado.
8. La aplicación permite la configuración de alerta automática para cambio de contraseñas en un período de tiempo definido antes de su expiración.
9. La aplicación permite el uso de autenticación centralizada (Directorio Activo).
10. Previo a la publicación de información desde la aplicación, la autenticación debe ser exitosa.
11. En caso de que no permita el uso de autenticación centralizada, permite la configuración de Políticas de Seguridad de la Información - PSI.
12. La Unidad requirente fue notificada del proceso de entrega y reseteo de credenciales.
13. Permite que la construcción de claves se apegue al estándar definido en la Institución.
14. La aplicación restringe el uso de las últimas cinco contraseñas utilizadas.
15. La aplicación permite el bloqueo de acceso al tercer intento fallido de sesión.
16. La aplicación permite el reseteo de contraseña luego del primer inicio de sesión.
17. La aplicación permite el cifrado de contraseñas.
18. La aplicación cuenta con el log de monitoreo para autenticación de usuarios activado.
19. No existen cuentas huérfanas creadas en la aplicación.
20. El área requirente fue notificada de que el acceso de usuarios externos es autorizado por Seguridades de la Información.
21. La aplicación está registrada en el inventario actualizado de aplicaciones.
22. La licencia de la aplicación está registrada en el inventario actualizado de licenciamiento de la Institución
23. El Catálogo de servicios fue actualizado.
24. La aplicación tiene publicado el acuerdo de responsabilidad del uso definido por la DGIP, que permite a un usuario aceptar de manera digital la responsabilidad del uso de la aplicación.
25. La aplicación permite el almacenamiento de los registros de identidad de los usuarios internos y externos que aceptaron el acuerdo de responsabilidad del uso definido por la DGIP en la aplicación, con las credenciales de logueo, y demás campos informativos que permitan realizar reportes de control de aceptación de este acuerdo.
26. La aplicación debe ser publicada bajo el dominio de la EPN utilizando certificados y protocolos de seguridad para la transmisión de datos (HTTPS, SSL 3.0 o TLS 1.0).
27. La aplicación obtuvo resultados positivos, es decir que no presenta vulnerabilidades de criticidad alta, que pongan en riesgo la confidencialidad, integridad y disponibilidad de la información que

es generada, procesada o transferida por la aplicación, tras la ejecución de pruebas de seguridad sobre la aplicación basadas en el TOP TEN DE OWASP.[3]

[3] Documento de los diez riesgos de seguridad más importantes en aplicaciones web según la organización OWASP (en inglés Open Web Application Security Project.