ANEXO X

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

1. OBJETIVO

Definir los criterios de seguridad que deben aplicarse durante el ciclo de vida de los aplicativos. Establecer un marco de desarrollo seguro a través de la implementación de ambientes independientes dentro del ciclo de vida de desarrollo de sistemas.

2. ALCANCE

Comprende a todos los sistemas y aplicativos informáticos, tantos desarrollos propios de la S.R.T. como de terceros.

3. DEFINICIONES

Aplicaciones: es un tipo de software que permite la interacción entre el usuario y la PC/equipamiento informático, permitiendo a éste elegir opciones y ejecutar acciones que el programa le ofrece.

Ambientes: Un ambiente refiere a hardware y software donde se ejecuta una aplicación. Dependiendo del proceso de desarrollo la cantidad de ambientes por los cuales iremos propagando una aplicación desde desarrollo hasta producción.

Base de datos: conjunto estructurado de datos de un mismo contexto, ordenado de modo sistemático para su posterior recuperación, análisis y/o distribución.

Ciclo de vida de desarrollo: es la estructura que contiene los procesos, actividades y tareas relacionadas con el desarrollo y mantenimiento de un producto de software, abarcando la vida completa del sistema, desde la definición de los requisitos hasta la finalización de su uso.

Enrutamiento: es el proceso de selección de rutas en cualquier red. Una red de computación está formada por muchas máquinas, y rutas o enlaces que las conectan. La comunicación en una red interconectada se puede producir a través de muchas rutas diferentes.

Protocolo: sistema de reglas que permiten que dos o más entidades se comuniquen entre ellas para transmitir información por medio de cualquier tipo de medio físico. Pueden ser implementados por hardware, software o una combinación de ambos.

Riesgo: potencial de que una amenaza específica explote las debilidades y pueda ocasionar una pérdida y/o daño a los activos. La medición de un riesgo se hace con la exposición, que se calcula como producto entre el impacto y la probabilidad de ocurrencia.

Software: el término se utiliza para referirse de una forma muy genérica al código de un dispositivo informático, sin embargo, éste abarca todo aquello que es intangible en un sistema informático.

Testing: es una actividad más en el proceso de control de calidad dentro del ciclo de vida. Refiere a las pruebas de software cuyo objetivo es proporcionar información objetiva e independiente sobre la calidad del producto a la parte interesada.

Transacción: es un grupo de operaciones que tienen las siguientes propiedades: atómicas, coherentes, aisladas y duraderas (ACID). La compatibilidad con transacciones permite desarrollar nuevos tipos de aplicaciones, al tiempo que simplifica el proceso de desarrollo y hace que la aplicación sea más sólida.

4. RESPONSABILIDADES

El Responsable de Seguridad de la Información (RSI) junto con la Subgerencia de Sistemas (S.S.) debe definir los controles de seguridad a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.

El RSI en conjunto a la S.S. definen los lineamientos de seguridad desde la fase inicial del proceso de adquisición o desarrollo de un sistema hasta su implementación o puesta en producción.

El RSI debe definir criterios a implementar con el fin de incorporarlos a la metodología de desarrollo utilizada.

La S.S. debe implementar los mecanismos necesarios para el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas. Asimismo, debe implementar los mecanismos necesarios para poder contar con una metodología de desarrollo seguro.

5. CONTENIDO

5.1 LINEAMIENTO DE SEGURIDAD EN LA ADQUISICIÓN Y DESARROLLO DE SOFTWARE

Se deberá garantizar que la seguridad sea una parte integral de los sistemas de información, desde la fase inicial del proceso de adquisición o el diseño de los mismos. Estos incluyen sistemas de operación, infraestructura, aplicaciones operativas, servicios y aplicaciones desarrolladas o adquiridas por la S.R.T..

5.1.1 Requerimiento de seguridad para adquisición de software

Para el caso que se considere la adquisición o tercerización del desarrollo de software, se deben establecer estrategias que contemplen los siguientes puntos:

- Acuerdos de licencias, propiedad de código fuente y derechos conferidos;
- Requerimientos respecto a la calidad y seguridad del código, y la existencia de garantías;
- Cláusulas que incluyan el cumplimiento de los requerimientos de seguridad del software establecido;
- Verificación del cumplimiento de las condiciones de seguridad establecidas por la S.R.T..

5.1.2 Controles de seguridad en el diseño para desarrollos propios de sistemas

Se deberán establecer controles respecto a la seguridad de la información en la etapa de análisis y diseño de los sistemas. Para esto, es necesaria la definición de una estrategia que incluya una etapa de evaluación de riesgos, para que se incluyan controles de seguridad a los requerimientos, de acuerdo al desarrollo a implementar y a la información que forma parte de dicho desarrollo.

5.1.3 Seguridad de la información en pliegos de bases y condiciones

Se deberán considerar todos los aspectos de seguridad relacionados al desarrollo de software, incorporando los mismos a cláusulas específicas en las especificaciones técnicas de los pliegos de bases y condiciones particulares.

5.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO

Se deberán incorporar en los nuevos sistemas de información y en todas las mejoras o actualizaciones a los ya existentes, las medidas de seguridad para el desarrollo de aplicaciones, la cuales serán aplicable a todos los desarrollos de sistemas de información de la S.R.T..

5.2.1 Requisitos de seguridad para un desarrollo seguro

Se deberá emitir criterio respecto de aquellos aspectos de seguridad necesarios en el desarrollo y puesta en producción del software, con el fin de poder incorporarlos a la metodología de desarrollo de la S.R.T., de manera tal que se considere a la seguridad de la información como parte del proceso. En estos criterios, se deberán incluir todos los puntos de control necesarios para asegurar que la aplicación puesta en producción cuente con las medidas necesarias relativas a la seguridad.

A tales fines, deberán contemplarse los requisitos de seguridad de identificación, autenticación, autorización, registración y trazabilidad durante todo el ciclo de vida del desarrollo del software.

Asimismo, se deberá capacitar periódicamente a todo el personal técnico que forma parte del ciclo de vida del software con el fin de promover el desarrollo seguro, pudiendo incluir:

- Revisión de derechos de acceso de los usuarios, determinando intervalos de revisión regulares;
- Estándares y prácticas de desarrollo seguro;
- Vulnerabilidades existentes y formas de mitigarlas desde el ciclo de desarrollo;
- Herramientas y metodologías que permitan generar un entorno más seguro;
- Prácticas de testing que permitan identificar posibles vulnerabilidades.

5.2.2 Seguridad en los entornos de desarrollo

Se deberán establecer medidas que favorezcan entornos de desarrollo seguros, relacionadas a la restricción de accesos al código fuente; la realización de copias de resguardo periódico; la utilización de entornos independientes de desarrollo y el establecimiento de procedimientos de pasaje de entornos.

5.2.3 Control de Cambios

Durante el ciclo de vida de desarrollo de software se deberán evaluar, validar y documentar los cambios realizados, mediante un versionado detallado con el objeto de minimizar los riesgos de modificaciones indebidas que pudieran comprometer las operaciones del entorno productivo, respetando las instancias de desarrollo, pruebas y producción.

5.2.4 Protección de datos en pruebas

Se deberán proteger los datos utilizados en las pruebas de desarrollo de software, evitando, en la medida de la posible, la utilización de bases de datos reales. Asimismo, se tendrá que evitar la utilización de datos extraídos del ambiente productivo, de modo de evitar exponer información que no sea pública para los casos que dicho requerimiento sea de aplicación.

En ese sentido, se deberá establecer una estrategia para la identificación de la información que se somete a pruebas para que, en aquellos casos que se deban utilizar datos reales, se cuente con los mecanismos necesarios que justifiquen su utilización y garanticen su empleo estrictamente para el fin perseguido.

5.2.5 Pruebas de Seguridad del Sistema

En ambientes de prueba se deberá evaluar la seguridad de las aplicaciones antes de ser incluidas en los ambientes de producción, especialmente aquellas que se gestionen a través de Internet.

5.3 SEGURIDAD EN LA TRANSMISIÓN DE INFORMACIÓN

5.3.1 Protocolos de transmisión o enrutamiento

Se deberán utilizar protocolos que garanticen la transmisión o enrutamiento adecuados en los servicios de aplicación, con el objeto de proteger y evitar la transmisión incompleta, alteración, pérdida, divulgación y/o duplicación no autorizada de mensajes o su reproducción.

Se deberá promover el uso de certificados y/o firma digital para garantizar las comunicaciones de extremo a extremo, la validación y verificación de autenticación en toda la cadena de transmisión, para garantizar la confidencialidad de las transmisiones y la utilización de protocolos seguros.

5.3.2 Protocolos para información gestionada por aplicaciones web

Se deberán tomar recaudos para garantizar la protección de la integridad de la información gestionada por aplicaciones web, a fin de prevenir accesos y/ modificaciones no autorizadas. Es por ello que se deberá prever para todos los sistemas que gestionen a través de Internet:

- La información se obtenga, procese y proporcione de acuerdo a la normativa vigente, en especial la Ley de Protección de Datos Personales;
- La información sensible o confidencial sea protegida durante el proceso de recolección y su almacenamiento;
- El acceso al sistema de publicación no permita el acceso accidental a las redes a las cuales éste se conecta;
- La/El responsable de la publicación de información en sistemas de acceso público sea claramente identificado y/o individualizado;
- La información se publique teniendo en cuenta las normas establecidas al respecto;
- Se garantice la validez y vigencia de la información publicada.

5.3.3 Seguridad en los servicios accedidos desde redes publicas

Se deberán implementar estrategias de seguridad para todos los sistemas del Organismo que se expongan a redes públicas, como Internet, con el objeto de evitar errores de enrutamiento, mensajes no autorizados, alteración de los datos, divulgación de la información, duplicación de mensajes o reproducción no autorizada entre otras amenazas. Dichas estrategias pueden incluir, entre otros, la aplicación de:

- Túneles de comunicaciones cifrados con protocolos seguros;
- Múltiples factores de autenticación;
- Uso de firma digital;
- Certificados digitales en los dos extremos.

5.4 ASPECTOS DE SEGURIDAD EN DESARROLLO DE TERCEROS

Se deberán establecer mecanismos de seguridad para controlar las actividades realizadas por el cocontratante en el caso de desarrollos llevados adelante por terceros para la S.R.T..

5.4.1 Control y supervisión al cocontratante

Se deberá establecer criterio con el fin de llevar a cabo el control y supervisión para el efectivo cumplimiento de la seguridad sobre las actividades realizadas por el cocontratante en aquellas contrataciones efectuadas por el Organismo relacionadas a desarrollos tercerizados.

República Argentina - Poder Ejecutivo Nacional
1983/2023 - 40 AÑOS DE DEMOCRACIA

Hoja Adicional de Firmas
Anexo firma conjunta

Número: IF-2023-66586118-APN-GT#SRT

CIUDAD DE BUENOS AIRES
Viernes 9 de Junio de 2023

Referencia: ANEXO X Adquisición, Desarrollo y Mantenimiento de Sistemas-EX-2023-56789749-APN-GT#SRT

El documento fue importado por el sistema GEDO con un total de 5 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:41:05 -03:00

Diego Maximiliano Segovia
Subgerente
Subgerencia de Sistemas
Superintendencia de Riesgos del Trabajo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:53:25 -03:00

Marcelo Angel Cainzos
Gerente
Gerencia Técnica
Superintendencia de Riesgos del Trabajo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:53:26 -03:00