IV Conferencia Científica Internacional
Universidad de las Ciencias Informáticas

Temática: Políticas, regulaciones, normativas, metodologías y estándares

Medidas de seguridad para protección de la información sensible en centros de desarrollo de software

Security measures to protect sensitive information in software development centers

Michel James Navarro[1]

[1] Dirección de Seguridad Informática, Universidad de las Ciencias Informáticas. Carretera a San Antonio de los Baños, Km. 2 ½. Torrens, municipio de La Lisa. La Habana, Cuba.

* Autor para correspondencia: mjames@uci.cu

Resumen

La información es fundamental dentro de los activos informáticos para cualquier organización, enfrentando diariamente numerosas amenazas de seguridad tanto internas como externas, poniendo en riesgo su integridad, disponibilidad y confidencialidad. En entidades cubanas, como empresas y universidades, estas amenazas se encuentran presente en sus áreas, incluidos los centros de desarrollo de software. Todas estas sedes tienen implementados Sistemas de Gestión de la Seguridad Informática (SGSI) a partir de las normativas de seguridad vigentes, pero no contemplan a fondo la protección de la información crítica. Para este trabajo se realizó una evaluación del estado de la seguridad informática y de los riesgos a los bienes informáticos que se necesita proteger para la selección de controles de específicos seguridad. El objetivo de la presente investigación consiste en realizar una propuesta de medidas de seguridad informática para la protección de la información sensible en los centros de desarrollo de software, a partir de los elementos obtenidos de la familia de normas ISO/IEC 27000 y los decretos y reglamentaciones que rigen la seguridad informática en Cuba.

Palabras clave: información sensible; medidas de seguridad informática; seguridad informática; centros de desarrollo de software; protección.

Abstract
Information is essential within computing assets for any organization, facing numerous internal and external security threats on a daily basis, jeopardizing its integrity, availability and confidentiality. In Cuban entities, such as companies and universities, these threats are present in their areas, including the software development centers. All these locations have Computer Security Management Systems (ISMS) implemented based on current security regulations, but do not fully cover the protection of critical information. For this work, an assessment was made of the state of computer security and of the risks to computer assets that need to be protected for the selection of specific security controls. The objective of this research is to make a proposal of computer security measures for the protection of sensitive information in software development centers, based on the elements obtained from the ISO/IEC 27000 standards family and decrees and regulations governing computer security in Cuba.

Keywords: *sensitive information; computer security measures; computer security; software development centers; protection.*

Introducción

Los ataques informáticos a nivel mundial acrecientan y los incidentes de seguridad informática se presentan con más frecuencia en todos los entornos. Debido a este incremento, es recomendable invertir en una buena gestión para la protección de los datos. Según (ISO/IEC 27002, 2017), la seguridad de la información se consigue mediante la implantación de un conjunto adecuado de controles, lo que incluye políticas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware. Los controles de seguridad son medidas de seguridad técnicas o administrativas para evitar, contrarrestar o minimizar la pérdida o falta de disponibilidad debido a las amenazas que actúan por una vulnerabilidad asociada a la amenaza. (ISO/IEC 27000, 2018)

Las empresas de desarrollo de software se enfrentan diariamente a numerosas amenazas de seguridad que ponen en riesgo la integridad, disponibilidad y confidencialidad de sus sistemas y de su información sensible. Este tipo de información es aquella, así definida por su propietario, cuya revelación, alteración, pérdida o destrucción puede producir daños importantes. (Alestra CERT, 2020)

Resulta evidente que los beneficios que se derivan del empleo de las tecnologías de la información sobrepasan en buena medida los inconvenientes y riesgos que a su vez traen asociados, razón por la cual éstas son aceptadas y no se discute la necesidad de su utilización (García Pierrat & Vidal Ledo, 2016). La empresa ESET en su reporte anual de amenazas (ESET, 2020) hace énfasis en las nuevas formas de trabajo que muchas organizaciones han tenido que adoptar en el primer trimestre del año. Enfrentar nuevos desafíos tecnológicos atrae a cibercriminales, los cuales rápidamente han ajustado sus estrategias para beneficiarse del cambio. Por su parte, en el último reporte "Global Data Risk Report From The Varonis Data Lab" (Varonis, 2019), se identificó un aumento de la información en riesgo con un 53% de las compañías con más de 1000 archivos sensibles accesibles sin ningún tipo de restricción. Para garantizar un nivel de seguridad deseado, es imprescindible prestar especial atención a los activos informáticos, siendo la información y los sistemas que la procesan, los activos fundamentales para cualquier entidad. Estos deben estar protegidos bajo controles, normas y políticas de seguridad como la forma efectiva, directa y profesional de comunicarse con los usuarios finales, ya que las mismas comprenden la forma de actuar del personal técnico, en relación con los recursos y servicios informáticos. (Abad, 2018)

Cuba plantea en sus lineamientos de la política económica y social del partido y la Revolución (VI Congreso del PCC, 2016), avanzar gradualmente en el proceso de informatización de la sociedad, el desarrollo de la infraestructura de telecomunicaciones y la industria de aplicaciones y servicios informáticos. A su vez propone sustentarlo en un sistema de ciberseguridad que proteja nuestra soberanía tecnológica y asegure el enfrentamiento al uso ilegal de las tecnologías de la información y la comunicación.

A pesar de que un nivel de seguridad absoluto no se pueda alcanzar debido a factores incontrolables, un buen sistema de gestión de la seguridad de la información puede lograr disminuir las amenazas y su impacto. Sobre esto (Montesino, 2012) plantea que el proceso de gestión de la seguridad informática requiere el establecimiento de gran cantidad de controles, la implementación de variados sistemas de seguridad con mecanismos de gestión independientes, y una elevada capacidad de respuesta ante los diversos ataques y vulnerabilidades existentes. Esto hace que el mismo sea complejo y en muchas ocasiones inefectivo, más aún cuando es posible que los ciber criminales combinen las vulnerabilidades para hacer el ataque posible o más peligroso. (Acunetix, 2020)

En las entidades cubanas, las amenazas contra los activos de la información se encuentran presentes en todas sus áreas, teniendo en muchas empresas y universidades centros de desarrollo de software. En estas sedes, los Sistemas de Gestión de la Seguridad de la Información (SGSI) implementados, están basados en las normativas de seguridad vigentes en el país, haciendo un análisis de riesgo personalizado, pero no contemplan a fondo la protección de la información sensible con todas sus aristas asociadas. El establecimiento de procedimientos correctamente definidos garantiza, además de la uniformidad en la aplicación de las políticas, la seguridad del cumplimiento de las mismas y su sistematicidad. (Ministerio de Comunicaciones, 2019)

En los centros de desarrollo de software de las distintas organizaciones nacionales, para la protección de los activos, se establecen controles de seguridad informática, estos se elaboran estableciendo cuál es la información más importante mediante el análisis de riesgos, determinando los que requieren de una atención especial desde el punto de vista de protección. Actualmente, los controles establecidos e implementados para regular la aplicación de medidas extras de seguridad a los activos informáticos, no son específicos ni están especializados. No contemplan a fondo la protección de la información sensible mediante la aplicación de la nueva legislación cubana y sus aristas asociadas con los estándares internacionales. Dentro de estos activos se encuentran la documentación de proyectos de producción de software, código fuente, sistemas informáticos, entre otros de vital importancia.

Estos controles están basados en la seguridad informática, dirigidos a prevenir, detectar y responder a las acciones que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce o conserva por medio de las TIC. A pesar de esto, los activos informáticos necesitan poner en práctica la seguridad de la información. Este término va más allá, integra toda la información independientemente del medio en el que esté. Provee de medidas de seguridad a otros medios donde se localice información como impresos en papel, discos duros, e incluso respecto a las personas que la conocen. (ISOTools Excellence, 2020)

Este trabajo tiene como objetivo presentar un conjunto de medidas enfocadas en el cumplimiento de las políticas de seguridad para la protección de la información sensible en todos sus formatos, a partir de las normativas internacionales, decretos y resoluciones nacionales que rigen la seguridad informática.

Materiales y métodos o Metodología computacional

Gestión de la Seguridad Informática

Un SGSI conlleva la conformación de una estrategia sobre cómo tratar los aspectos de seguridad e implica la implementación de los controles necesarios para garantizar el cumplimiento de lo establecido en esta materia, a partir de un análisis de riesgos. Este proceso se encuentra descrito en la norma certificable a nivel internacional ISO/IEC 27001, y ofrece un modelo para su diseño, implementación, operación, monitorización, revisión y mejora continua.

Con respecto a la implantación de la seguridad informática, la Resolución 129 del Ministerio de Comunicaciones (Ministerio de Comunicaciones, 2019) plantea que generalmente todas las entidades que emplean las TIC en el desarrollo de su actividad, tienen implementadas determinadas normas, medidas y procedimientos de seguridad, generalmente de forma empírica a partir de incidentes que han ocurrido o de las experiencias de otras entidades. Es necesario evaluar de manera crítica la efectividad de los controles existentes, sobre la base de los resultados del análisis de riesgos realizado, con el objetivo de perfeccionarlos o sustituirlos por aquellos que brinden la respuesta adecuada. Los resultados de esta evaluación ayudan a orientar y a determinar una apropiada acción gerencial y las prioridades para gestionar los riesgos de seguridad informática, así como la implementación de los controles seleccionados para protegerse.

Selección de controles de seguridad informática

Utilizando las normas ISO/IEC 27001, ISO/IEC 27002 y las legislaciones cubanas, como referencia para seleccionar controles dentro del proceso de implantación de un SGSI, se realiza la propuesta de controles para la reducción de los riesgos en los centros de desarrollo de software. Los controles de seguridad informática son considerados en las etapas de especificación de requisitos y de diseño de sistemas y aplicaciones. El no hacerlo puede dar lugar a costos adicionales y a soluciones menos eficaces, y en el peor de los casos, imposibilidad de alcanzar la seguridad adecuada. Estos controles son establecidos, implementados, supervisados y mejorados cuando sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad de la organización. Hay que tener presente que ningún sistema de controles puede alcanzar la seguridad completa y que acciones adicionales de gestión se implementan para supervisar, evaluar, y mejorar la eficiencia y la eficacia de los controles de seguridad para apoyar las metas de la organización. (Ministerio de Comunicaciones, 2019)

La selección de estos controles depende de una decisión organizacional basada en los criterios para la aceptación del riesgo, y está conforme a las regulaciones nacionales y las normativas internacionales vigentes. La seguridad informática se logra implantar con un conjunto adecuado de controles, que incluyen políticas, procesos, medidas, procedimientos, estructuras organizativas y funciones de hardware y software. Para la protección de la información sensible en los centros de desarrollo de software se seleccionaron como controles, las medidas, como complemento a las políticas implantadas para asegurar el objetivo este trabajo.

Medidas de Seguridad Informática

La Metodología para la Gestión de la Seguridad Informática en Cuba, establece que las medidas y procedimientos de seguridad que se implementen en correspondencia con las políticas definidas, conforman el cuerpo del sistema de seguridad diseñado y representan la línea de defensa básica de protección de los bienes informáticos, por lo que es sumamente importante su selección adecuada, de forma tal que cubran las amenazas identificadas durante el proceso de evaluación de riesgos, y se implementen de una manera rentable.

La seguridad es implementada mediante el establecimiento de múltiples barreras de protección, la selección de controles de diferentes tipos de forma combinada y concéntrica, para lograr una determinada redundancia que garantice que, si una medida falla o resulta vulnerada, la siguiente medida entre en acción y continúe la protección del activo o recurso. No es conveniente que el fallo de un solo mecanismo comprometa totalmente la seguridad. La implementación de múltiples medidas simples puede en muchos casos ser más seguro que el empleo de una medida muy sofisticada.

Disposiciones de seguridad informática

Disposiciones Internacionales

Norma ISO/IEC 27001: Especifica los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información en el contexto de la organización. También incluye los requisitos para la apreciación y el tratamiento de los riesgos de seguridad de la información a la medida de

las necesidades de la organización. Los requisitos que establece son genéricos y aplicables a todas las organizaciones, cualquiera que sea su tipo, tamaño o naturaleza. (ISO/IEC 27001, 2017)

Norma ISO/IEC 27002: Tiene como principal objetivo establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Esto también incluye la selección, implementación y administración de controles, teniendo en cuenta los entornos de riesgo encontrados en la empresa. Está diseñada para que las organizaciones la usen como referencia a la hora de seleccionar controles dentro del proceso de implantación de un SGSI basado en la norma ISO/IEC 27001, o bien como documento guía para organizaciones que implanten controles de seguridad de la información comúnmente aceptados. (ISO/IEC 27002, 2017)

Disposiciones nacionales

Decreto No. 360/2019: El objeto de este Decreto es establecer el marco legal que ordene el empleo seguro de las Tecnologías de la Información y la Comunicación, para la informatización de la sociedad, la defensa del Ciberespacio Nacional en correspondencia con lo establecido en la Constitución, las leyes y las restantes disposiciones legales relacionadas con el tema, así como los tratados y demás instrumentos jurídicos internacionales de los que la República de Cuba es Estado parte. Tiene como objetivo establecer los niveles de seguridad en correspondencia con los riesgos asociados a la evolución de las TIC y las posibilidades reales de enfrentar estos últimos. (Consejo de Ministros, 2019)

Resolución 128/2019: Aprueba el Reglamento de seguridad de las Tecnologías de la Información y la Comunicación. Tiene por objeto complementar las disposiciones del Decreto 360 "Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional" de 5 de junio de 2019, y establecer las funciones de los sujetos que intervienen en esta, así como garantizar un respaldo legal que responda a las condiciones y necesidades del proceso de informatización del país. Su objetivo es minimizar los riesgos sobre los sistemas informáticos y garantizar la continuidad de los procesos informáticos. (Ministerio de Comunicaciones, 2019)

Resolución 129/2019: Aprueba la metodología sobre la gestión de la seguridad informática en todo el país. Tiene por objeto determinar las acciones a realizar en una entidad durante el diseño, la implementación y posterior operación de

un Sistema de Gestión de la Seguridad Informática, compuesta por dos partes, la primera se dedica al SGSI y la segunda a la estructura y contenido del Plan de Seguridad Informática. (Ministerio de Comunicaciones, 2019)

Resultados y discusión

A partir de los mínimos requisitos de seguridad, se elaboraron las Medidas. Tienen como base la combinación de los estándares y normativas de seguridad analizados, enfocados a la protección de la información sensible. De cada uno la investigación obtuvo los elementos necesarios para conformar las medidas analizando sus puntos de encuentro.

Medidas de seguridad para la protección de la información sensible

Las medidas elaboradas están agrupadas en categorías principales de controles de seguridad. Según (ISO/IEC 27002, 2017), en función de las circunstancias, todos los controles de seguridad pueden ser importantes y el orden de la lista de controles no implica orden de prioridad. A continuación, se relacionan las 44 medidas obtenidas a partir del estudio:

Organización de la seguridad

1. Los Centros heredan las políticas de seguridad informática aprobadas por su entidad principal.
2. Todas las responsabilidades de seguridad informática se deben definir y asignar.
3. La seguridad de la información se debe tratar dentro de la gestión de proyectos.
4. Se debe garantizar la seguridad en el uso de dispositivos móviles utilizados para el trabajo.
5. Se debe garantizar la seguridad en el teletrabajo.

Seguridad relativa a los recursos humanos

6. A los trabajadores se le debe exigir que conozcan su responsabilidad de seguridad de la informática y la apliquen de acuerdo con los controles establecidos en la organización.
7. Todos los trabajadores y personas involucradas en el proyecto, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre políticas y procedimientos, según corresponda a su puesto de trabajo.

8. Debe existir un proceso disciplinario formal que recoja las medidas a tomar ante aquellos que hayan incurrido en alguna violación de seguridad informática.
9. Los intereses del Centro y la Entidad deben protegerse en el proceso de cambio o finalización del empleo.

Gestión de activos

10. Los activos informáticos del área deben identificarse y asignarles un responsable.
11. Todos los trabajadores deben devolver los activos de la Entidad que estén en su poder al finalizar su empleo, contrato o acuerdo.
12. La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante la revelación o modificación no autorizadas.
13. Todos los soportes de almacenamiento deben ser comprobados antes de deshacerse de ellos para confirmar que la información sensible se ha eliminado de manera segura o destruirlos en caso de ser necesario.
14. Se debe asegurar la información contenida en los activos en movimiento.

Control de acceso

15. Se debe establecer, documentar y revisar la política de control de acceso basada en los requisitos de negocio y seguridad de la información.
16. Se debe garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.
17. El acceso a la información y a las funciones de las aplicaciones debe ser restringido de acuerdo con la política de control de acceso definida.

Criptografía

18. Se debe garantizar un uso adecuado y eficaz de la criptografía para proteger la información.

Seguridad física

19. Las áreas o zonas controladas deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
20. Se debe diseñar y aplicar una protección física contra desastres naturales, ataques intencionados o accidentes.
21. Los equipos se deben situar de forma que se reduzcan los riesgos de las amenazas humanas y ambientales, así como las oportunidades de que se produzcan accesos no autorizados.

22. Los equipos críticos deben estar protegidos contra fallos de alimentación y otras alteraciones eléctricas.
23. Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad e integridad continuas.
24. Los activos informáticos no deben sacarse de las instalaciones del Centro sin previa autorización.
25. Los usuarios deben asegurarse que el equipo desentendido tiene la protección adecuada.
26. Deben mantenerse los puestos de trabajo despejado de papeles y medios de almacenamiento extraíbles y una pantalla limpia de información sensible.

Seguridad de las operaciones

27. Se deben controlar todos los cambios en el Centro, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afecten a la seguridad de la información.
28. Los recursos de desarrollo, pruebas y operación se deben separar para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.
29. Se deben implementar controles de detección, prevención y recuperación que sirvan de protección contra el código malicioso.
30. Se deben realizar copias de seguridad de la información sensible y verificarla periódicamente.
31. Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información en los sistemas internos del área.
32. Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición del Centro a dichas vulnerabilidades y adoptar medidas adecuadas para afrontar el riesgo asociado.
33. La instalación de software por parte de los usuarios debe ser restringida para evitar la introducción de vulnerabilidades y otros incidentes de seguridad.
34. Las redes inalámbricas en los locales con requerimientos específicos se deben controlar según la importancia de los bienes informáticos que contienen y su utilización.
35. Se deben establecer controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.

Desarrollo y mantenimiento de los sistemas de información

36. Se deben establecer y aplicar reglas dentro del proyecto para el desarrollo seguro de aplicaciones y sistemas.

37. Las aplicaciones críticas del proyecto se deben revisar y probar cuando se realicen modificaciones a los sistemas operativos para garantizar que no existen efectos adversos en las operaciones o la seguridad.
38. Se deben establecer y proteger adecuadamente los entornos para el desarrollo de las aplicaciones y sistemas.
39. Se deben seleccionar adecuadamente los datos de prueba, protegerlos y controlarlos.

Gestión de Incidentes

40. Se debe implementar un sistema de gestión de incidentes de seguridad informática.
41. Se debe responder adecuadamente ante los incidentes de seguridad informática.
42. Se deben utilizar el conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad informática para reducir la probabilidad o el impacto de los incidentes en el futuro.

Cumplimiento

43. El SGSI del Centro debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.
44. Se debe garantizar que la seguridad de la información se implementa y se opera de acuerdo con el reglamento, políticas, normas y cualquier otro requisito de seguridad aplicable.

Conclusiones

Teniendo en cuenta que la información y los sistemas que la procesan son los activos más importantes para cualquier entidad, es indispensable protegerlos de amenazas bajo controles de seguridad informática. Estos deben cubrir adecuadamente las necesidades específicas de las entidades. Su selección, para asegurar que los riesgos se reduzcan a un nivel aceptable, está basada en los criterios para la aceptación del riesgo, las opciones para su tratamiento, el acercamiento a su gestión general aplicada a la organización, y también está conforme con toda la legislación y regulaciones nacionales e internacionales vigentes.

Las medidas elaboradas proporcionan una barrera de protección importante en los centros de desarrollo de software. Su desarrollo a partir de la combinación de la familia de normas internacionales ISO/IEC 27000 y las disposiciones nacionales que rigen la seguridad informática, brinda solides y alcance para la protección de la información sensible. Se definieron a partir de una evaluación de riesgos para proporcionar un adecuado nivel de protección a todos los

bienes informáticos. Estos controles servirán como base para la creación de procedimientos específicos que establezcan en detalle los pasos requeridos para proteger el sistema informático, y dentro de este, la información crítica de las organizaciones.

Referencias

1. Ministerio de Comunicaciones. Resolución 129 de 2019 de Ministerio de Comunicaciones. La Habana : Gaceta Oficial de la República de Cuba, 2019.

2. ISO/IEC 27001. Information technology. Security techniques. Information security management systems. Requirements. s.l. : International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), 2017.

3. ISO/IEC 27002. Information technology. Security techniques. Code of practice for information security. s.l. : International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), 2017.

4. Ministerio de Comunicaciones. Resolución 128 de 2019 de Ministerio de Comunicaciones. La Habana : Gaceta Oficial de la República de Cuba, 2019.

5. Consejo de Ministros. Decreto 360 de 2019 de Consejo de Ministros. La Habana : Gaceta Oficial de la República de Cuba, 2019.

6. Montesino, Perurena Raydel. Modelo para la gestión automatizada e integrada de controles de seguridad informática. La Habana : s.n., 2012.

7. ESET. Threat Report Q1 2020. s.l. : ESET, 2020.

8. Varonis. Global Data Risk Report From The Varonis Data Lab. 2019.

9. VI Congreso del PCC. Actualización de los lineamientos de la política económica y social del Partido y la Revolución para el período 2016-2021. La Habana : s.n., 2016.

10. ISOTools Excellence. SGSI. Blog especializado en Sistemas de Gestión. [En línea] 18 de Julio de 2020. https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/.

11. Análisis y estudio de políticas de seguridad informática para un ISP con usuarios residenciales. Abad, Cesar Remigio Vega. 2018, PRO SCIENCES: REVISTA DE PRODUCCIÓN, CIENCIAS E INVESTIGACIÓN, Vol. 2, págs. 32-38. E-ISSN: 2588-1000.

12. La informática y la seguridad. Un tema de importancia para el directivo. García Pierrat, Gonzalo y Vidal Ledo, María Josefina. 2016, INFODIR, págs. 47-58. 1996-352.

13. ISO/IEC 27000. Information technology. Security techniques. Information security management systems. Overview and vocabulary. s.l. : International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)., 2018.

14. Acunetix. Web Application Vulnerability Report 2020. 2020.

15. Alestra CERT. Alestra CERT. [En línea] 20 de 07 de 2020. https://alestracert.com.mx/boletines/necesidades-de-la-informacion-sensible/.