Nombre del instituto: Instituto Tecnológico de Tlalnepantla

Carrera: Ingeniería en tecnologías de la información y comunicación

Materia: Tecnologías de la seguridad en software

Profesor: Hilda Diaz Rincón

Nombre de los alumnos: Diana Godínez Roblero & Zúñiga Morales Noé

Grupo: T-92

Actividad: ACTIVIDAD 2. DIA 24 MAYO A7-A9 ISO27002

Contenido

Introducción

A7. Seguridad relativa a los recursos, A8. Gestión de activos y A9. Control de acceso de la ISO 27002 nos ayudan a implementar sistemas de seguridad de información o mejorar los ya existentes en el laboratorio de cómputo, la zona de cómputo de la biblioteca y el departamento de servicios escolares del Instituto Tecnológico de Tlalnepantla.

Selección de departamentos

Para la actividad 2 se tomará la opción 1 y se seleccionará para aplicar en el laboratorio de cómputo, zona de cómputo de la biblioteca y servicios escolares.

7. Seguridad relativa a los recursos de la información

7.1 Antes del empleo

Objetivo:

Para asegurarse que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.

7.1.1 Investigación de antecedentes

Control:

Comprobación de los antecedentes de los candidatos al puesto de trabajo debe de llevarse de acuerdo a las leyes, normativas y códigos éticos que sean de aplicación, debiendo ser proporcionales a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos

Implementación:

Los candidatos deberán probar que la información presentada en su currículum vitae es verídica y cumplen con las competencias necesarias para desarrollar roles en seguridad, ya que la información que manejan los departamentos seleccionados es de estado crítico.

7.1.2 Términos y condiciones del empleo

Control:

Como parte de las actividades contractuales, los empleados y contratistas debe establecer términos y condiciones en contrato de trabajo en que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.

Implementación:

Todo el personal que accedan a información sensible deberá firmar un compromiso de confidencialidad y no revelación previa a que les sea otorgado el acceso a los recursos. Los empleados tendrán la responsabilidad de clasificar y gestionar la información de los departamentos en los que se desempeñen.

7.2 Durante el empleo

Objetivo:

Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad informática

Control:

La dirección exige a los empleados, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.

Implementación:

El personal será debidamente informado de sus responsabilidades a seguridad de la información previamente a brindarles el acceso a información sensible, demostrando apoyo a políticas y controles de seguridad de la información dentro de los departamentos.

7.2.2 Concienciación, educación y capacitación en seguridad de la información

Control:

Todos los empleados de la organización y, cuando corresponda, los contratistas, deberían recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.

Implementación:

Programas de concienciación diseñados de acuerdo a las funciones del personal en sus respectivas áreas, debiendo incluirse actividades que brinden información respecto a nuevas políticas y procedimientos de seguridad relevantes de forma regular.

8. Gestión de activos

8.1 Responsabilidad sobre los activos

Objetivo:

Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.

8.1.1 Inventario de activos

Control:

La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deberían estar claramente identificados y debería elaborarse y mantenerse un inventario.

Implementación:

Se enlistarán todos los inventarios tomando en cuenta cuales de estos manejan información sensible para el funcionamiento del área, así como activos que involucren información sobre estudiantes y personal de la institución.

8.1.3 Uso aceptable de los activos

Control:

Se deberían identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.

Implementación:

Establecer un reglamento de uso para el uso de los activos tomando en cuenta la integridad de los mismas y las tareas designadas a cada área en función del horario y el uso de los activos estará restringido por control parental.

8.2 Clasificación de la información

Objetivo:

Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.

8.2.1 Clasificación de la información

Control:

La información debería ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.

Implementación:

La información solo será manejada por personal autorizado y esta se encontrará protegida por contraseña y será clasificada de acuerdo a que área pertenece.

8.2.3 Manipulado de la información

Control:

Debería desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.

Implementación:

De acuerdo a la clasificación hecha en el punto 8.2.1 se establece quien tiene acceso a la información de acuerdo a cada área.

8.3 Manipulación de los soportes

Objetivo:

Evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en soportes.

8.3.2 Eliminación de soportes

Control:

Los soportes deberían eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.

Implementación:

Eliminar los soportes escritos por medio de la destrucción de los mismos de tal forma que la información de estos sea inteligible, además de mezclarse y separarse en contenedores diferentes.

9 control de acceso

9.1 Requisitos de negocio para el control de acceso

Objetivo:

Limitar el acceso a los recursos de tratamiento de información y a la información

9.1.1 Política de control de acceso

Control:

Se debería establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.

Implementación:

El personal tendrá acceso solo a la información que le corresponde, acorde a su puesto y departamento. Solo podrán acceder a información de otros departamentos con permisos extendidos por los encargados de estos.

9.1.2 Acceso a las redes y a los servicios de red

Control:

Únicamente se debería proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados

Implementación:

El personal tendrá acceso solo a las redes de la escuela, ya que son las más seguras, cada uno de los equipos contara con procedimientos de autorización que otorguen el permiso de conexión a red, de igual forma los servicios serán monitoreados para que se tenga un mejor desempeño.

9.2 Gestión de acceso de usuarios

Objetivo:

Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.

9.2.1 Registro y baja de usuarios

Control:

Deberán implementarse procedimientos formales de registro y retirada de usuarios que hagan posible la asignación de los derechos de acceso

Implementación:

Identificación de usuarios por medio de identificadores ID, cada uno deberá hacerse responsable de las actividades que se realicen bajo el registro de su ID, para todo personal que deje el departamento o la organización, su ID será dado de baja de forma inmediata

9.2.4 Gestión de la información secreta de autenticación de los usuarios

Control:

La asignación de la información secreta de autenticación debería ser controlada a través de un proceso formal de gestión.

Implementación:

Todos los usuarios que hagan uso de la información de los departamentos seleccionados, deberán acordar mantener confidencialidad de la información, apoyando con su autenticación personal (credencial estudiantil o de docencia), al

termino del uso de la información seleccionada o deberán confirmar la recepción de esta

9.2.5 Revisión de los derechos de acceso de usuario

Control:

Los propietarios de los derechos de acceso deberían revisar los derechos de acceso de usuario a intervalos regulares

Implementación:

Revisiones regulares de los derechos de acceso del personal, siendo reasignados cuando este cambie de departamento o área, los derechos de acceso privilegiados también serán revisados frecuentemente.

9.3 Responsabilidades del usuario

Objetivo:

Se debería requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.

9.3.1 Uso de la información secreta de autenticación

Control:

Se debería requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.

Implementación:

Antes de acceder a información se debe de presentar un documento que acredite su persona (credencial escolar de preferencia) y naturaleza de lo que realizara (por ejemplo, un oficio)

Conclusión Noé

En conclusión, el uso de las normas ISO 27001 y 27002, no es algo rígido a seguir si no que es más una recomendación, pues es flexible para usar por separado, es decir se pueden utilizar apartados sin necesidad de ponerla completamente

Conclusión Diana

El conocimiento de las Normas ISO 27001 e ISO 27002 nos ayudan a entender como aplicarlas y desarrollarlas adecuadamente para poder obtener una certificación. Para el trabajo que empezamos a desarrollar nos ayudan a pensar que en todas las implantaciones que hagamos debemos incluirlas, es decir, debemos pensar que la actividad debe tener una calidad que se acerque a la autorización de una fase inicial de auditoría

Bibliografía

Industria Conectada 4.0 - Normas UNE-EN ISO/IEC 27001 y UNE-EN ISO/IEC 27002 para la seguridad de la información. (2022). Retrieved May 25, 2022, from Industriaconectada40.gob.es website: https://www.industriaconectada40.gob.es/difusion/noticias/Paginas/Normas-UNE-EN-ISOIEC-27001-UNE-EN-ISOIEC-27002-seguridad-de-informaci%C3%B3n.aspx