UNIVERSIDAD DEL CENTRO DEL BAJIO.

LICENCIATURA EN SISTEMAS COMPUTACIONALES.

TÍTULO:

“ESQUEMAS Y MODELOS DE SEGURIDAD”.

MATERIA:

SEGURIDAD INFORMATICA.

DOCENTE:

FILIBERTO DURAN GARCIA.

PRESENTA

PABLO SÁNCHEZ UGALDE.

Celaya, Guanajuato , 02 de Febrero del año 2019.

Misión de seguridad.

Ofrecer soluciones y servicios en seguridad informática con el principal objetivo de ayudar a nuestros clientes a proteger su información.

El objetivo de la seguridad informática es mantener la Integridad, Disponibilidad, Privacidad, Control y Autenticidad de la información manejada por computadora.

Aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información.

Integridad.

Los componentes del sistema permanecen inalterados a menos que sean modificados por los usuarios autorizados.

Disponibilidad.

Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen.

Privacidad.

Los componentes del sistema son accesibles sólo por los usuarios autorizados.

Control.

Solo los usuarios autorizados deciden cuando y como permitir el acceso a la información.

Autenticidad.

Definir que la información requerida es válida y utilizable en tiempo, forma y distribución.

No Repudio.

Evita que cualquier entidad que envió o recibió información alegue, que no lo hizo.

Auditoria.

Determinar qué, cuándo, cómo y quién realiza acciones sobre el sistema.

Políticas de seguridad.

La seguridad informática es en sí mismo un concepto amplio y diverso que abarca numerosas derivadas. La seguridad se puede centrar en la prevención de ataques y situaciones de riesgo para los sistemas de una organización o hacerlo más en los mecanismos de mitigación de los efectos que un ataque pueda ocasionarle a una empresa o particular. Si tuviéramos que definir qué son las políticas de seguridad informática podríamos empezar negando aquello que no son, es decir, afirmar que no son una descripción técnica de mecanismos ni una suerte de código penal que sancione, y al mismo tiempo conduzca, la labor de los empleados. Por el contrario, sí que tienen que ver con una descripción amplia, basada en objetivos globales, de los bienes y valores que deseamos proteger y la motivación de dicho deseo.

Así, ante la cuestión planteada –qué son las políticas de seguridad informática– se han manejado tradicionalmente distintas definiciones y todas ellas tienen en común su carácter restrictivo, en la medida en que limitan la actuación de los empleados durante la operación general del sistema y también su alto nivel de abstracción, de modo que vienen a ser más que nada una declaración de intenciones, un asentamiento de las bases que deben definir y delimitar las responsabilidades en las distintas actuaciones que se requerirán en caso de amenaza o ataque. En cualquier caso, estas políticas van a tener su concreción en toda una serie de normas, protocolos, reglamentos, convenciones… en las que, principalmente, se fijará el modo de comunicación con los usuarios y también entre los empleados.

Cómo debe ser una política de seguridad informática eficaz

Antes de definir qué son las políticas de seguridad informática, hay que saber que para ser eficaces deben reunir una serie de características relacionadas con su holismo, es decir, aspirar a cubrir todos los aspectos, su capacidad de adaptación a las necesidades de cada organización y a los recursos de que se dispone y, por último, ser atemporal, en el sentido de que debe ser susceptible

de ser aplicada en cualquier momento. Además, cualquier política de seguridad debe incorporar y contemplar elementos claves como la integridad de los programas, su disponibilidad, la privacidad de las operaciones y los archivos y, finalmente, ejercer un control eficaz y efectivo, garantizar la autenticidad de las comunicaciones y los protocolos y ser útil, pues ninguna medida coercitiva se justifica a sí misma si no es en virtud del principio de utilidad.

Principios de las políticas de seguridad informática.

Por último, insistir en que más allá de saber qué son las políticas de seguridad informática, lo verdaderamente relevante es conocer cuáles son los principios que rigen estas políticas y que terminan haciéndolas eficaces. Así, es esencial fijar un principio de responsabilidad individual, unas reglas claras de autorización (quién y de qué forma puede emplear los recursos), partir del mínimo privilegio (cada uno puede usar únicamente lo imprescindible para llevar a cabo su trabajo), la separación de las obligaciones, en el sentido de que las tareas deben estar divididas entre las diferentes personas relacionadas con la actividad o función reduciendo las posibilidades de sufrir un ataque; el de auditoría, que remarca que todas las actividades y los recursos requeridos deben ser monitoreados desde el inicio y hasta finalizado el proceso, y el de redundancia o énfasis en la realización de copias de seguridad creadas cada poco tiempo y almacenadas en lugares distintos.

Referencia.

ANÓNIMO

En el texto: (2019)

Bibliografía: (2019). Retrieved from https://www.uv.mx/personal/llopez/files/2011/09/presentacion.pdf

¿QUÉ SON LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA?

En el texto: ("¿Qué son las políticas de seguridad informática?", 2019)

Bibliografía: ¿Qué son las políticas de seguridad informática?. (2019). Retrieved from https://www.segurode.com/noticias/ciberriesgos/valor-politicas-seguridad-informatica