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 del alumno: Noé Zúñiga Morales

Grupo: T-92

Actividad: 3.1 Controles en Aplicaciones en producción

Introducción

Los controles de aplicación son esos controles o revisiones que corresponden al alcance de las aplicaciones o procesos de comercio, que integran la versión de datos para comprobar su precisión, la diferenciación de las funcionalidades de comercio, el registro de las transacciones, la generación del detalle de errores, entre muchos, los controles de aplicación son las revisiones que efectúan las organizaciones en el campo de la auditoría interna, para afirmar que cada transacción sea manejada conforme el objetivo específico de control, el control de aplicación se relaciona con los datos y transacciones que efectúa cada sistema de aplicación, a fin de asegurar la exactitud e totalidad de los registros, la validez y resultado de los procesos de cada programa.

Índice

1.- Control Interno Informático

1.1.- Aspectos clave del control interno

excesivo énfasis en la Gestión (eficiencia y efectividad) descuidando Controles incrementa el riesgo de errores e irregularidades

Gestión: Cuando la balanza está desbalanceada hacia el lado de la gestión se afecta el control, cuando esto pasa es usualmente en el sector privado
Control: Cuando la balanza está desbalanceada hacia el lado del control se afecta la gestión, cuando esto pasa es usualmente en el sector público

Administración y auditoría deberían trabajar de acuerdo a sus roles in los dos lados de la balanza, sin embargo, a veces ellos prefieren/deciden trabajar solo en un lado, y cunado esto pasa es usualmente de esta manera:

- ADMINISTRACIÓN. - extremadamente enfocado en gestión sin considerar controles
- AUDITORÍA. - extremadamente enfocado en controles sin considerar gestión

Equilibrio Entre Riesgos y Controles	
Los componentes de la aceptación de riesgos excesivos:	Consecuencias de la implementación de controles excesivos:
• Pérdida potencial de activos • Toma de decisiones de negocios incorrecta o ineficaz • Incumplimiento potencial con las leyes y regulaciones • Posibilidad de que se cometan fraudes	• Aumento de la burocracia • Exceso del costo de producción • Complejidad innecesaria de los controles • Incremento del tiempo de ciclo • Actividades que no agregan valor

- La Administración: Corrige errores y/o reitera y replica aciertos
- La Administración: Planifica la gestión y el control de la organización
- La Administración: Evaluación de la gestión y el control; permanente, por parte de quien hace el proceso, con menor independencia y objetividad (Self Assessment).
- Auditoría: Evaluación de la gestión y el control; periódica, por parte de quien conoce el proceso, con mayor independencia y objetividad.
- La Administración: Ejecuta la gestión y el control de la organización

Mejoramiento Continuo
ADMINISTRACIÓN

- Permanente
- Por quien hace y conoce el proces
- Menos independiente y objetiva

Monitoreo continuo
AUDITORÍA

- Periódica

- Por quien conoce el proceso
- Más independiente y objetiva

1.2.- CONTROL INTERNO

Proceso que lleva a cabo el control diario de todas las actividades de la operación sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la dirección de la organización, así como los requerimientos legales.

1.2.1.- OBJETIVOS DEL CONTROL INTERNO

1. Promover la efectividad y eficiencia en las operaciones incluyendo la salvaguarda de activos
2. Asegurar a razonabilidad
3. Soportar el cumplimiento son las leyes y regulaciones aplicables

1.2.2.- RESPONSABILIDADES FRENTE AL SISTEMA DE CONTROL INTERNO

1.3.- CONTROL INTERNO INFORMÁTICO

Se refiere a realizar en los diferentes sistemas (centrales, departamentales, redes locales, PC's, etc.) y entornos informáticos (producción, desarrollo o pruebas) el control de las diferentes actividades operativas.

1.3.1.- OBJETIVOS PRINCIPALES

- Controlar que todas las actividades en los sistemas que se realizan cumplan los procedimientos y normas establecidos, evaluar sus beneficios y asegurarse del cumplimiento de normas legales.
- Asesorar sobre el conocimiento de las normas.
- Colaborar y apoyar el trabajo de Auditoria informática, así como de las auditorías externas al grupo.
- Definir, implantar y ejecutar mecanismos y controles para comprobar el logro del servicio informático.

1.3.2.- TIPOS DE CONTROL INTERNO

En el ambiente informático, el control interno se materializa fundamentalmente en controles de dos tipos:

- Controles manuales.
- Controles automáticos.

1.3.2.1.- Controles manuales

Aquellos que son ejecutados por el personal del área usuaria o de informática sin la utilización de herramientas computacionales.

1.3.2.2.- Controles automáticos

Son generalmente los incorporados en el software, llámense estos de operación, de comunicación, de gestión de base de datos, programas de aplicación, etc.

1.3.3.- CATEGORÍAS DE CONTROL INTERNO

De acuerdo a su finalidad se clasifican en:

- Controles preventivos.
- Controles detectivos.
- Controles correctivos.

1.3.3.1.- Controles preventivos

Para tratar de evitar un hecho, como un software de seguridad que impida los accesos no autorizados al sistema.

1.3.3.2.- Controles detectivos

Cuando fallan los preventivos para tratar de conocer cuanto antes el evento

1.3.3.3.- Controles correctivos

Facilitan la vuelta a la normalidad cuando se ha producido incidencias

1.4.- AUDITORÍA INFORMÁTICA Y CONTROL INTERNO

DIFERENCIAS	
CONTROL INTERNO INFORMATICO	AUDITOR INFORMÁTICO
Realizada por auditores internos o externos	Análisis en un momento determinado
Informa a la Dirección del Departamento de Informática (Gobierno TI)	Informa a la Dirección General de la Organización
Realizada por la administración de TI	Realizada por auditores internos o externos.

1.5.- ASPECTOS DE IMPLANTACIÓN EN UN SISTEMA DE CONTROL INFORMÁTICO

Para la implantación de un sistema de controles internos habría que definir:

- Gestión de sistema de información
- Administración de sistemas.
- Seguridad
- Gestión del cambio

1.5.1.- Gestión de sistema de información
Políticas, pautas y normas técnicas que sirvan de base para el diseño y la implantación de los sistemas de información y de los controles correspondientes.

1.5.2.- Administración de sistemas
Controles sobre la actividad de los centros de datos y otras funciones de apoyo al sistema, incluyendo la administración de las redes.

1.5.3.- Seguridad
incluye las tres clases de controles fundamentales implantados en el software del sistema, integridad del sistema, confidencialidad (control de acceso) y disponibilidad.

1.5.4.- Gestión del cambio
separación de las pruebas y la producción a nivel del software y controles de procedimientos para la migración de programas software aprobados y probados.

1.6.- Áreas de Aplicación del Control Interno Informático

- Controles generales organizativos
- Controles de desarrollo, adquisición y mantenimiento de sistemas de información.
- Controles sobre las aplicaciones
- Controles sobre la administración de sistemas de información.
- Controles sobre específicas tecnologías.
- Controles de Calidad

1.7.- CONTROLES GENERALES ORGANIZATIVOS

- Políticas
- Reglamentos
- Manuales e Instructivos.
- Formatos
- Estándares
- Procedimientos
- Descripción de funciones y responsabilidades
- Informes de Control

1.8.- CONTROLES DE DESARROLLO, ADQUISICIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACION

- Metodología del ciclo de vida del desarrollo de sistemas
- Explotación y mantenimiento.

1.9.- CONTROLES SOBRE APLICACIONES

- Control de entrada: Datos completos, exactos, válidos y autorizados por única vez.
- Control de tratamiento de datos: procesamiento de las transacciones es completa, adecuado y autorizado
- Control de salida de datos: Presentación completo de los resultados

1.10.- CONTROLES SOBRE LA ADMINISTRACIÓN DE LOS SISTEMAS DE INFORMACIÓN

- Planificación y gestión de los recursos informáticos.
- Controles para usar de manera efectiva los recursos en ordenadores
- Revisiones técnicas sobre equipos de infraestructura.
- Procedimientos y formatos de selección del software del sistema, de instalación, de mantenimiento, de seguridad y de control de cambios.
- Seguridad física y lógica

1.11.- CONTROLES ESPECIFICOS SOBRE TECNOLOGÍAS

- Controles en servicios informáticos.
- Controles centralizados de ordenadores personales
- Controles conexiones con host y redes de área local.

1.12.- CONTROLES DE CALIDAD

- Normas de documentación de programas
- Normas de pruebas de programas
- Normas con respecto a pruebas de sistemas
- Pruebas pilotos o en paralelo
- Evaluación del cumplimiento del software.

1.13.- CONTROL INTERNO MODELOS INTERNACIONALES

Se han publicado diversos **modelos** de **Control**, así como numerosos lineamientos para un mejor gobierno corporativo. Los **modelos** más conocidos son:

- COSO (USA)
- COCO (Canadá)
- Cadbury (Reino Unido)
- Vienot (Francia)
- Peters (Holanda)
- King (Sudáfrica)
- MICIL (adaptación del COSO para Latino- américa).

1.13.1.- INFORME COSO

Coso I

- Se creó en 1992.
- Evalúa y Mejora el sistema de control interno en las entidades

Coso II

- Se creó en 2004
- Es un marco integrado sobre análisis de riesgo.

Coso III

- Se creó en 2013
- Es una actualización y mejora de COSO I

1.13.2.- INFORME COSO III- Definición

Es un marco de referencia o modelo común de control interno contra el cual las empresas y organizaciones pueden evaluar sus sistemas de control interno.

1.13.3.- INFORME COSO III

Objetivos

- Establecer una definición común de control interno que responda a las necesidades de las distintas partes.
- Facilitar un modelo en base al cual las empresas y otras entidades, cualquiera sea su tamaño y naturaleza, puedan evaluar sus sistemas de control interno.

Ambiente de Control	• Demostrar compromiso con la integridad y los valores éticos • Ejercer la responsabilidad de supervisión • Establecer la estructura, la autoridad y la responsabilidad • Demostrar compromiso con las competencias • Aplicar la rendición de cuentas
Evaluación de Riesgo	• Especificar objetivos adecuados • Identificar y analizar los riesgos • Evaluar el riesgo de fraude • Identificar y analizar cambios significativos
Actividades de Control	• Seleccionar y desarrollar actividades de control • Seleccionar y desarrollar controles generales sobre la tecnología • Implementación a través de políticas y procedimientos
Información & Comunicación	• Utilizar información pertinente • Comunicación interna • Comunicación externa
Actividades de Monitoreo	• Realizar evaluaciones continuas y / o separadas • Evaluar y comunicar las deficiencias

2.- LA PLANEACION Y EVALUACION DE LOS PROCESOS PRODUCTIVOS

Dos conceptos son importantes en la planeación y evaluación de los procesos productivos:

- Costo de los insumos y materia prima al realizar el producto.
- Beneficio que se obtendrá al vender este producto.

Por ello es necesario comprar insumos de buena calidad para que nuestro producto sea adquirido por la gente y así obtengamos un beneficio que en nuestro caso serán las ganancias generadas por las ventas. Si compro insumos de regular o mala calidad, tendremos que vender nuestros productos a un bajo costo y por lo tanto el beneficio que obtendremos será poco.
¿En qué momento debemos considerar estos conceptos?, pues en la planeación ya que en este momento se determinan los objetivos que pretendemos alcanzar, se diseña el proceso, se eligen los insumos, se definen las técnicas para la elaboración del producto y se genera la documentación necesaria.
La corrección se efectúa mediante la intervención adecuada.

2.1.- La evaluación como parte de la resolución de problemas técnicos y el trabajo por proyectos en los procesos productivos

La evaluación como parte de la resolución de problemas técnicos y el trabajo por proyectos en los procesos productivos
Cuando se requiere desarrollar una solución técnica para un problema, hay que organizar las acciones que deben efectuarse a partir de la información que se tiene del problema o la necesidad, con el propósito de evaluar las distintas soluciones técnicas que pueden aplicarse.
Un proceso de producción es un sistema de acciones que se encuentran interrelacionadas de forma dinámica y que se orientan a la transformación de ciertos elementos.
De esta manera, los elementos de entrada conocidos como factores pasan a ser elementos de salida productos, tras un proceso en el que se incrementa su valor.
Cabe destacar que los factores son los bienes que se utilizan con fines productivos las materias primas. Los productos, en cambio, están destinados a la venta al consumidor o mayorista.

3.- Entornos existentes en el ciclo de desarrollo de software y despliegue de aplicaciones

Una vez que empezamos a planificar una aplicación o una página web, requerimos 2 entornos: desarrollo y producción. La máquina de desarrollo suele ser nuestro propio ordenador en el cual programaremos todo nuestro código. Por otro lado, poseemos el ámbito de producción, que usaremos una vez que queramos desplegar nuestra aplicación y hacerla pública.

No obstante, acorde pasa la época vamos necesitando más espacios: un comprador puede necesitar un ámbito para pruebas y testing, los accesorios de desarrolladores un ámbito de pre-producción o staging, el QA un ámbito para descubrir bugs, etcétera.

3.1.- Entorno de desarrollo

En el entorno de desarrollo se programa el software. Puede haber diferentes opciones: el propio ordenador del programador o incluso un servidor compartido por los desarrolladores para que creen la aplicación.
Este entorno debe parecerse lo máximo posible al entorno de producción, por no decir que debe ser igual.

3.2.- Entorno de testing

Es en este entorno en el que se ejecutan los tests y se realizan las pruebas de una determinada funcionalidad que hayamos desarrollado. De la misma manera que el entorno de desarrollo, este entorno debe parecerse al máximo al entorno de producción.

3.3.- Entorno UAT: User Acceptance Testing

Las pruebas de aceptación de usuario (User Acceptance Testing) forman la última fase de un proceso de pruebas. En este entorno, usuarios reales realizan pruebas para asegurarse de que los requisitos de desarrollo de software se han cumplido, es decir, que los desarrolladores han hecho una funcionalidad tal y como se ha pedido y el software es completamente usable.
Esta es una de las fases más importantes en el ciclo de desarrollo de software porque así nos aseguramos de que el usuario final está contento con el resultado.

3.4.- Entorno de pre-producción o staging

El entorno de pre-producción o staging es, como su propio nombre indica, el último entorno al que vamos a desplegar nuestra aplicación antes de que vaya a producción.
En este entorno, lo mejor sería que además de tener la misma configuración software que en el entorno de producción, tuviésemos también la misma configuración hardware. De esta manera, un QA podría identificar errores incluso de rendimiento.

3.5.- Entorno de producción

Este entorno ya es accesible a todo el mundo. Si hemos configurado todos nuestros entornos de la misma manera, realizado pruebas exhaustivas del software, tests automatizados y seguido buenas prácticas, no deberíamos tener ningún problema en el despliegue. Y si lo tuviéramos, simplemente tendríamos que comenzar de nuevo el ciclo de desarrollo: código, pruebas y despliegue.

4.- Seguridad en aplicaciones

Cada vez las aplicaciones poseen más grandes funciones y dan más grande ingreso a la información sensible del comercio, sin embargo, la rapidez a la que crece esta información en la mayor parte de las empresas sobrepasa su capacidad de protegerla y gestionarla.
Se ha estimado que el precio por vulnerabilidad en la fase de desarrollo es de alrededor de $500 dólares, en lo que en la etapa de pruebas llega a $7,000 dólares y en la etapa de producción alcanza los $14,000.

La mayoría de las vulnerabilidades encontradas en una prueba de hacking ético deben ser resueltas y revalidadas, sobre todo las críticas. Sin embargo, los estudios indican que en un alto porcentaje no se resuelven correctamente, generando una falsa sensación de seguridad.
Por otro lado, la naturaleza de estas pruebas conlleva una serie de problemas

- Pueden existir vulnerabilidades en las aplicaciones pero que no hayan sido encontradas por los expertos (hackers éticos).
- Puede haber vulnerabilidades no cubiertas por el alcance de las pruebas ya sea por falta de tiempo o de presupuesto.
- Asimismo, pueden existir nuevas vulnerabilidades que se hayan descubierto o publicado después de haber sido realizado el estudio.
- Pueden producirse nuevas vulnerabilidades que se hayan introducido a nivel código en el desarrollo evolutivo o correctivo de las aplicaciones.

4.1.- Cómo lograr seguridad en las aplicaciones

la estabilidad en las aplicaciones se consigue por medio de un enfoque integral que considere la conjunción de una secuencia de recursos complementarios como por ejemplo puntos tecnológicos, organizacionales y normativos.

Tendrá que considerarse la relación entre diversas zonas de la organización en medio de las que por lo menos tienen que estar la de estabilidad, de desarrollo, de operaciones y de bases de datos.

El enfoque tendrá que ser gradual, explicando alcances específicos para cada etapa de tal forma que se garantice que en todas ellas se se incrementa escalonadamente el grado de estabilidad.

Al final se debería tener en cuenta que esta clase de iniciativas toman tiempo por lo cual se tienen que proponer proyectos de extenso plazo con adelantos seguidos y constantes.

4.1.1.- Evaluación aplicativa

El primer factor a tener en cuenta es la evaluación continua de cada una de y todas las aplicaciones, tomando en cuenta primero esas que son más críticas. Para eso se necesita empezar con un inventario actualizado de cada una de las aplicaciones incluyendo variantes, actualizaciones, parches, configuraciones, etcétera.

4.1.2.- Sensibilización y formación

Es imprescindible sensibilizar a cada una de las piezas interesadas sobre la realidad de los peligros determinados en la fase de evaluación aplicativa y transmitir evidentemente la necesidad de mitigarlos.

Además, se debería mejorar la formación de los equipos de estabilidad y desarrollo. O sea, los profesionales en estabilidad tienen que saber más sobre las aplicaciones y el periodo de vida de desarrollo de sistemas (SDLC) y las zonas de desarrollo deben saber bastante más de estabilidad y considerarla una sección integral del proceso SDLC. En resumen, aprender “Desarrollo Seguro”. Según Fortify la formación en buenas prácticas de desarrollo seguro puede reducir un 25% la introducción de vulnerabilidades a grado código.

4.1.3.- Desarrollo seguro

Uno de los recursos clave para poder hacer la estabilidad aplicativa es la utilización de buenas prácticas en el desarrollo para que las aplicaciones sean seguras por diseño, a partir de las etapas iniciales del SDLC (requerimientos) hasta las pruebas y puesta en producción. Incluyendo la asignación de los papeles de arquitectura de estabilidad y el de diseño de estabilidad aplicativa.

Se debería tener en cuenta además la evaluación automatizada de vulnerabilidades a grado código. Deberán existir políticas que impidan la puesta en producción de aplicaciones que no hayan sido plenamente probadas.

4.1.4.- Arquitectura de seguridad

Al final como parte de la arquitectura de estabilidad de las aplicaciones, se deberán tener en cuenta los controles normativos a llevar a cabo así como los controles tecnológicos (incluyendo productos comerciales) a llevar a cabo; primordialmente firewalls aplicativos y de base de datos para tener visibilidad del tráfico aplicativo y poder diferenciar lo cual es legítimo de lo cual no lo es.

Además es fundamental que los conjuntos de operaciones cuenten con recursos de monitoreo que les permitan saber lo que pasa con las aplicaciones.

5.- SERIES DE LIDERAZGO DE SEGURIDAD: Estrategias de seguridad para el éxito

5.1.- 5 PASOS PARA CONTROLAR APLICACIONES Y DATOS

5.1.1.- Centrarse en el equilibrio entre las necesidades de seguridad y de la experiencia de usuario

Cuando las aplicaciones y los datos susceptibles permanecen amenazados, la estabilidad debería preponderar sobre la facilidad de ingreso y facilidad de uso.
Dicho esto, las empresas de éxito toman una perspectiva holística de la estabilidad que se esfuerza en llevar a cabo controles de estabilidad no obstructivos y prácticas que no frustrarán innecesariamente a los usuarios ni dificultarán su productividad. Afortunadamente, varias de las defensas de estabilidad más efectivas son transparentes y fluidas para los usuarios finales.

5.1.2.- Habilitar opciones flexibles de almacenamiento de datos, acceso y gestión

Las organizaciones tienen la posibilidad de beneficiarse de manera considerable de tener una plantilla que es móvil o extensamente dispersa. Inevitablemente, no obstante, usuarios, dispositivos y sistemas dispersos e interconectados otorgan más fines a los atacantes cibernéticos. Las organizaciones requieren diseñar e implementar tácticas de administración de datos en consonancia con el costo y la confidencialidad de los datos en peligro. Para sus datos más confidenciales y críticos, ejemplificando, las empresas tienen la posibilidad de dictaminar que el almacenamiento únicamente se permita en sus servidores centrales más seguros, evitando la distribución fuera de los muros de la compañía e imponiendo estrictos requisitos y métodos de ingreso.

5.1.3.- Ofrezca un poderoso motor de políticas para controles contextuales

En sitio de ofrecer a los usuarios pases de ingreso total a sus datos, aplicaciones y redes, debería llevar a cabo controles que puedan tener en cuenta el entorno de cada solicitud de ingreso. Con estos controles, los administradores de TI tienen la posibilidad de entablar políticas que determinen los títulos y apartamentos de la gente, sus ubicaciones, la estabilidad de las redes que permanecen usando, las habilidades de sus terminales, e inclusive cambiantes tales como la hora del día en que tratan de entrar a los datos.

5.1.4.- Ofrezca un poderoso motor de políticas para controles contextuales

A grado mundial, las empresas se combaten a más de 300 regulaciones y leyes en relación con los niveles mínimos de privacidad y estabilidad, con bastante más de 3500 controles específicos actualmente. Para asegurar el cumplimiento y saciar las solicitudes de auditoría, las resoluciones de estabilidad tienen que dar una supervisión completa y automatizada, registro e informes de ingreso a datos, desplazamiento de datos y ocupaciones a grado de red. Es fundamental que las resoluciones sean lo suficientemente flexibles para ajustarse de forma fácil a las nuevas regulaciones y estándares mientras surgen.

5.1.5.- Reducir la superficie de ataque mientras bajan los costes de TI

Controlando el reparto de datos y proporcionando acceso contextual, las empresas tienen la posibilidad de minimizar significativamente sus áreas de ataque. Estas protecciones deben integrar la utilización rutinaria del cifrado de las aplicaciones y datos en reposo, en uso, o en tránsito. Paralelamente, con menos objetivos expuestos a defender, las organizaciones tienen la posibilidad de minimizar sus costes operativos ahorrándose compras de tecnologías de estabilidad centradas en dispositivos particulares

5.2.- 5 MEJORES PRÁCTICAS PARA HACER DE LA SEGURIDAD UN ASUNTO DE TODOS

5.2.1.- Educar a los usuarios

Una plantilla laboral informada, consciente de la seguridad es la primera línea de defensa de cada empresa contra amenazas a la seguridad, por lo tanto, enseñar a la gente cómo trabajar de forma segura desde cualquier lugar en cualquier dispositivo debe ser una prioridad. Enseñar las mejores prácticas es una buena receta contra el fracaso.

5.2.2.- Compromiso con las líneas de negocio de las organizaciones

Las estrechas relaciones laborales entre los ejecutivos de TI y los responsables de las líneas de negocio son un ingrediente esencial para una seguridad efectiva. Reunirse regularmente con los responsables de la toma de decisiones empresariales permite a los responsables de seguridad incorporar salvaguardias adecuadas a nuevas iniciativas empresariales desde el principio. También les da una perspectiva cercana e indispensable sobre los riesgos y los requisitos únicos de un grupo empresarial.

5.2.3.- Vea las políticas de seguridad de forma moderna y móvil

la formación por si sola no garantiza una seguridad fuerte. Muchos de los dispositivos, redes y sistemas de almacenamiento en los que los empleados confían hoy en día están fuera del control de TI.
revisar las políticas de seguridad para reflejar riesgos tales como almacenar datos del negocioen dispositivos propiedad del personal, publicando las contraseñas en un monitor de un ordenador, o utilizando un dispositivo de almacenamiento USB que encontró en el suelo.

5.2.4.- Aplique las políticas de forma apropiada y constantemente

Las políticas de seguridad pueden perder valor con el tiempo si los usuarios no creen que el violarlas tiene consecuencias, o peor aún, si creen que saltándoselas mejora la productividad. Las políticas deben ser mantenidas y actualizadas con el negocio. Los responsables de seguridad por lo tanto deben hacer cumplir las políticas de manera apropiada y consistentemente.

5.2.5.- Automatizar la seguridad correctamente

Muchas soluciones de seguridad pueden implementar comportamientos deseados tales como cifrado de datos del negocio en los dispositivos móviles de forma predeterminada. Pueden también construir una seguridad más estricta en los elementos fundamentales de la experiencia del usuario evitando automáticamente que los empleados utilicen aplicaciones no autorizadas sobre la red de la empresa o limitando qué aplicaciones pueden utilizar para archivos adjuntos de correo electrónico, por ejemplo. Otras soluciones proporcionan la funcionalidad de un registro e informes que le ayudarán a demostrar a los auditores que ha aplicado escrupulosamente las políticas adecuadas.

5.3.- 3 ESTRATEGIAS PARA ADMINISTRAR LOS MANDATOS DEL CUMPLIMIENTO NORMATIVO

5.3.1.- Permita el acceso al mismo tiempo que protege la información

Adoptar un planteamiento integral para la gestión de la identidad y el acceso, combinado con un profundo enfoque en los datos confidenciales e informes relevantes y métricas es un importante equilibrio. Las políticas deberían especificar los privilegios del acceso elemental a los datos dependiendo de dónde se encuentran los empleados, en qué red están y qué dispositivo están usando, con controles adicionales acordes con el riesgo.

5.3.2.- Controlar la información confidencial

La mayor parte de mandatos de seguridad se aplican principalmente a información personalmente identificable, archivos médicos, transacciones de pago y otros datos secretos. Para cumplir con estos mandatos, debe identificar primero los datos confidenciales creando un modelo de clasificación para las distintas clases de información que su la compañía crea, transmite, y almacena.

5.3.3.- Auditar, medir y demostrar el cumplimiento de la normativa

Los informes de seguridad integral son siempre importantes, pero son cruciales cuando se trata del cumplimiento normativo. Satisfacer esas demandas lleva un registro de conexión sistemático, informes y rigurosos procesos de auditoría suficientes para seguir cuando determinados usuarios acceden a aplicaciones y datos específicos, y son lo suficientemente flexibles para abordar nuevas regulaciones y estándares según aparecen. Crear también una consola de informes donde los responsables autorizados puedan ver el último cumplimiento de objetivos y resultados.

6.- Controles para sistemas informáticos en operación

Un sistema de control, a partir de las superficies de la ingeniería y la informática es un grupo complejo de recursos que se desempeñan como controladores de otros sistemas. Su finalidad primordial es llevar a cabo eficaz y verdaderamente los procesos para los cuales ha sido programado; caracterizándose por su comportamiento estable frente a los errores y pues las cambiantes de salida proceden acorde a las directivas dadas por las cambiantes de ingreso.

Históricamente, las primeras adaptaciones fundamentadas en un sistema de control datan de la vieja Grecia, una vez que se inventaron mecanismos para regular una plataforma flotante. Otro instante histórico de los sistemas de control es el reloj de Ktesibios que según registros data del año 250 anterior a cristo.

Los sistemas de control más frecuentes son: sistemas de control de lazo abierto y sistemas de control de lazo cerrado

6.1.- Sistemas de control de lazo abierto

En los sistemas de control de lazo abierto la señal de salida no afecta la operatividad del sistema total. Como sucede en un horno microondas que no tiene sensor de temperatura, el sistema de control de lazo abierto logra calcular automáticamente el tiempo y el grado de cocción.

6.2.- Sistemas de control de lazo cerrado

Los sistemas de control de lazo cerrado ejercen un proceso de realimentación que tiene la capacidad de transformar la señal para que esta se encuentre en función de la señal de salida; debido a esto la toma de decisiones no está subordinada totalmente a la entrada, sino que también depende de la salida.

Actualmente los sistemas de control son de gran importancia para la optimización de procesos, ya que poseen habilidades para solucionar o resolver informaciones automatizadas. Los podemos encontrar en multiplicidad de sectores económicos, en procesos de producción al emplear un equipo o manejar una máquina.

7.- Controles para aplicaciones

7.1.- ¿Qué es el control de aplicación?

El control de aplicación es proporcionado por un software que impide que las aplicaciones utilizadas por los empleados realicen acciones que puedan poner la red corporativa o el equipo en riesgo. Además, registra las acciones ejecutadas por las aplicaciones y gestiona las actividades realizadas por ellos de acuerdo con la política de seguridad establecida para el mismo.
Con el control de aplicación, las aplicaciones se clasifican en cuatro grupos:

7.1.1 Confiables
aplicaciones con firma digital de proveedores confiables.

7.1.2 Baja restricción
aplicaciones que no tienen una firma digital de un proveedor de confianza y recibieron un valor bajo de clasificación de amenaza.

7.1.3 Alta restricción
aplicaciones que no tienen una firma digital y tienen un valor alto de clasificación de amenaza.

7.1.4 No confiables
aplicaciones sin firma digital y que recibieron un valor muy alto de clasificación de amenazas.

7.2.- ¿Qué ventaja genera?

- El objetivo general del control de aplicación es asegurarse de que los datos que transitan a través de la red y entre las aplicaciones permanecen siempre protegidos y seguros.
- Mantiene malwares afuera de la red privada, permitiendo que la productividad y el ancho de banda no se vean afectados;
- Permite el bloqueo de cientos de aplicaciones de una forma fácil y rápida;
- Posibilita la creación de reglas personalizadas que se pueden agregar a cualquier protocolo no compatible;
- Facilita la creación de políticas basadas en el tiempo de uso de las aplicaciones;
- Emite informes que permiten a los administradores ver qué protocolos están activos en la red privada y quién los utiliza.

Bibliografia

Glenda Rivas Márquez. (2012). Modelos contemporáneos de control interno. Fundamentos teóricos. *Observatorio Laboral Revista Venezolana*, *4*(8), 115–136. http://servicio.bc.uc.edu.ve/faces/revista/lainet/lainetv4n8/art6.pdf

Instituto Tecnológico de Tlalnepantla (n.d.). Cursos2.Tlalnepantla.tecnm.mx. Retrieved April 11, 2022, from http://cursos2.tlalnepantla.tecnm.mx/pluginfile.php/191975/mod_assign/introattachment/0/Control_Interno_Informatico%20%282%29.pdf?forcedownload=0

Mario Pérez Esteso. (2019, June 13). *Entornos existentes en el ciclo de desarrollo de software y despliegue de aplicaciones*. Geeky Theory; Geeky Theory. https://geekytheory.com/entornos-existentes-ciclo-desarrollo-software-despliegue-aplicaciones-testing-produccion/

Polanco, M. (2019). *Seguridad en aplicaciones*. Magazcitum. https://www.magazcitum.com.mx/index.php/archivos/537#.X878lGhKhPY

citrix. (n.d.). Series de liderazgo de seguridad: Estrategias de seguridad para el éxito. In *citrix*. Retrieved April 11 C.E., from https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/security-leadership-series-security-strategies-for-success-es.pdf

virtualpro. (2019, August 27). *Control de sistemas: ejemplos y aplicaciones*. VirtualPro.co. https://www.virtualpro.co/noticias/control-de-sistemas--ejemplos-y-aplicaciones

Caso de estudio