SISAP
Sistemas Aplicativos

Riesgo y Cumplimiento
Ingeniero Antonio Cabrera

PROYECTO DE PRACTICA
MARCOS DE SEGURIDAD

Alexa Carolina Bravo
Octubre, 2022

INDICE

INTRODUCCIÓN

La ciberseguridad es un tema del cual aprendí un montón en el transcurso de este año, desde la parte teórica hasta la parte práctica. Es un tema con mucho campo y que nos rodea en el día a día, muchas veces sin darnos cuenta. Tener conocimiento sobre la seguridad es muy importante, más en estos tiempos, que la tecnología va avanzando constantemente. La ciberseguridad no solo se relaciona con lo tecnológico, también tiene relación con distintas áreas, como psicología, lo cual es bastante interesante y nos crea una manera nueva de pensar. En el siguiente trabajo se detalla la parte teórica que contiene la pagina web, realizada como proyecto de práctica, del área de riesgo y cumplimiento. En la pagina se puede encontrar información general sobre que es ciberseguridad. Información general sobre marcos de ciberseguridad, recomendaciones de material audiovisual relacionados con ciberseguridad y que nos invitan a realizar un análisis sobre como somos victimas potenciales de los ciberataques. Además de incluir información sobre siete marcos de ciberseguridad. La pagina web se realizó en react desde cero. Espero que sea lo suficientemente informativa para las personas que la visiten.

MARCO TEORICO

CIBERSEGURIDAD

¿Qué es la ciberseguridad?

Es la práctica de proteger sistemas, redes y programas de ataques digitales. Se le conoce también como seguridad de la tecnología de la información (TI), las medidas de ciberseguridad están diseñadas para combatir las amenazas a sistemas en red y aplicaciones, que se originan tanto desde dentro como desde fuera de una organización.

Actualmente, la implementación de medidas de seguridad digital se debe a que hay más dispositivos conectados que personas, y los atacantes son cada vez más creativos.

La ciberseguridad cuenta con tres pilares, los cuales son:

1. **Confidencialidad:** mantener los secretos y garantizar que solo los usuarios autorizados puedan obtener acceso a sus archivos y cuentas.
2. **Integridad:** garantizar que su información es la que debe ser y de que nadie ha insertado, modificado o eliminado cosas sin su permiso.
3. **Acceso:** garantizar que puede tener acceso a su información y sistemas cuando lo necesite.

Ciber amenazas más comunes

- **Suplantación de identidad/Phishing/ Ingeniería Social:** El phishing es una forma de ingeniería social que engaña a los usuarios para que proporcionen su propia información personal o información confidencial. Ocurre al enviar correos electrónicos fraudulentos que se asemejan a correos electrónicos de fuentes de buena reputación. Es el tipo más común de ciberataque.
- **Ransomware:** Es un tipo de software malicioso. Está diseñado para exigir dinero mediante el bloqueo del acceso a los archivos o el sistema informático hasta que se pague un rescate. El pago del rescate no garantiza que se recuperen los archivos o se restaure el sistema. Los últimos ataques de ransomware se han dirigido a gobiernos estatales y locales, que son más fáciles de quebrantar que las organizaciones y están bajo mayor presión a la hora de pagar rescates para restaurar las aplicaciones y sitios web en los que confían los ciudadanos.
- **Malware:** es un tipo de software diseñado para obtener acceso no autorizado o causar daños en una computadora, se refiere a variantes de software malicioso, como gusanos, virus, troyanos y spyware. El malware cada vez tiene más ataques "sin archivos" y están diseñados para eludir los métodos de detección más comunes, como las herramientas antivirus, que exploran los archivos adjuntos para detectarlos.

- **Ataques de intermediarios (Man in the Middle):** es un tipo de ataque donde un ciberdelincuente intercepta y retransmite mensajes entre dos partes para robar datos.
- **Ataques de denegación de servicio distribuido (DDoS):** intenta hacer caer un servidor, un sitio web o una red sobrecargándola con tráfico, generalmente desde varios sistemas coordinados. Los ataques DDoS agobian las redes empresariales a través del protocolo simple de gestión de red (SNMP), utilizado para módems, impresoras, conmutadores, routers y servidores.
- **Amenazas persistentes avanzadas (APT):** es cuando un intruso o un grupo de intrusos se infiltran en un sistema y permanecen sin ser detectados durante un largo período de tiempo. El intruso deja intactas las redes y sistemas para poder espiar la actividad empresarial y robar datos confidenciales evitando así que se activen contramedidas defensivas.

Tips de seguridad

- **Actualizar el software y el sistema operativo:** esto significa que aprovechará las últimas revisiones de seguridad.
- **Utilizar software antivirus:** las soluciones de seguridad detectarán y eliminan las amenazas. Mantenga su software actualizado para obtener el mejor nivel de protección.
- **Utilizar contraseñas seguras:** asegúrese de que sus contraseñas no sean fáciles de adivinar.
- **No abrir archivos adjuntos de correos electrónicos de remitentes desconocidos:** podrían estar infectados con malware.
- **No hacer clic en los vínculos de los correos electrónicos de remitentes o sitios web desconocidos:** es una forma común de propagación de malware.
- **Evitar el uso de redes Wi-Fi no seguras en lugares públicos:** las redes no seguras lo dejan vulnerable a ataques del tipo "Man-in-the-middle".

MARCOS DE CIBERSEGURIDAD

¿Qué es un marco de ciberseguridad?

Es un conjunto predefinido de políticas y procedimientos definidos por las principales organizaciones de seguridad cibernética para mejorar las estrategias de seguridad cibernética dentro de un entorno empresarial, y está documentado para el conocimiento teórico y los procedimientos de implementación práctica.

Los marcos de ciberseguridad a menudo se usan de manera obligatoria o al menos con fuertes incentivos en las empresas que desean cumplir con regulaciones estatales, industriales y de ciberseguridad internacional

Están diseñados para una industria específica y están creados para reducir las vulnerabilidades desconocidas y las configuraciones incorrectas que existen dentro de una red empresarial.

Implementación

Luego de identificar el marco de ciberseguridad adecuado, se debe realizar lo siguiente:

1. Las empresas primero necesitan probar e identificar la postura de seguridad actual dentro de su entorno
2. Analizar los proyectos existentes, el proceso involucrado en estos proyectos y los recursos involucrados con ellos.
3. Comprender el marco de ciberseguridad leyendo los documentos.
4. Distinguir qué controles de seguridad existen y no existen dentro de la red empresarial
5. Comunicar dónde se están retrasando las capas de seguridad y definir un plan para establecer el mismo
6. Implementar lo mismo en un marco de tiempo definido para mantener todo en orden y tiempo
7. Resaltar los controles que superan a los controles definidos por el marco
8. Discutir todo el plan con los actores clave, incluidos los interesados, y continúe con la implementación
9. Auditar el progreso de la implementación continuamente.
10. Generar informes y realizar reuniones para medir los desafíos.
11. Documentar todo el proceso de auditorías y otros beneficios.

Ventajas

- Los marcos de seguridad cibernética y sus políticas pueden superponerse entre sí, lo que permite a las organizaciones cumplir con múltiples marcos con el mínimo esfuerzo.
- Ciberseguridad mejorada.
- Mejor protección de datos
- Fácil cumplimiento y gestión de auditoría.

Desventajas

- La implementación puede llevar días, afectando la productividad.
- Una implementación incorrecta puede llevar a lagunas de seguridad
- Se pueden aplicar limitaciones financieras

Tipos de marcos de ciberseguridad

CIS Controls

¿Qué es?

CIS Controls son un conjunto priorizado de Salvaguardas para mitigar los ataques cibernéticos más frecuentes contra sistemas y redes. Están mapeados y referenciados por múltiples marcos legales, regulatorios y de políticas. CIS Controls v8 se ha mejorado para mantenerse al día con los sistemas y software modernos. El cambio a la computación basada en la nube, la virtualización, la movilidad, la subcontratación, el trabajo desde casa y las tácticas cambiantes de los atacantes impulsaron la actualización y respaldan la seguridad de una empresa a medida que avanzan hacia entornos híbridos y totalmente en la nube.

¿Cómo se implementa?

Los Controles de Seguridad Crítica de CIS son un conjunto prescriptivo y prioritario de mejores prácticas en seguridad cibernética y acciones defensivas que pueden ayudar a prevenir los ataques más peligrosos y de mayor alcance, y apoyar el cumplimiento en una era de múltiples marcos.

Control 1: Inventario y control de activos de hardware: Supervise activamente y gestione todos los dispositivos de hardware conectados a su red. Mantenga un inventario actualizado de todos sus activos tecnológicos y disponga de un sistema de autenticación para garantizar que los dispositivos no autorizados no tengan acceso a su red.

Control 2: Inventario y control de activos de software: Disponga de un sistema de inventario de software para supervisar y gestionar activamente todo el software que se esté ejecutando en su red. Utilice la lista blanca de aplicaciones para garantizar que sólo se instale y ejecute software autorizado y que se bloquee el software no autorizado.

Control 3: Gestión continua de vulnerabilidades: Analice continuamente sus activos para identificar posibles vulnerabilidades y remediarlas antes de que se conviertan en un problema. Fortalezca la seguridad de su red garantizando que el software y los sistemas operativos utilizados en su organización ejecuten las actualizaciones de seguridad más recientes.

Control 4: Uso controlado de los privilegios administrativos: Monitoree los controles de acceso y el comportamiento de los

usuarios de las cuentas privilegiadas para evitar el acceso no autorizado a los sistemas críticos. Garantice que sólo las personas autorizadas tengan privilegios elevados para evitar el uso indebido de los privilegios administrativos.

Control 5: Configuración segura para el hardware y el software de los dispositivos móviles, laptops, estaciones de trabajo y servidores: Establezca y mantenga configuraciones de seguridad basadas en los estándares de configuración aprobados por la organización. Defina un riguroso sistema de gestión de configuraciones que monitoree y alerte sobre las configuraciones erróneas e implemente un proceso de control de cambios para impedir que los atacantes se aprovechen de los servicios y configuraciones vulnerables.

Control 6: Mantenimiento, monitoreo, y análisis de logs de auditoría: Recopile, gestione y analice los logs de auditoría de los eventos para detectar anomalías. Mantenga registros de log para comprender los detalles de los ataques a fin de responder a los incidentes de seguridad de manera eficaz.

Control 7: Protección de correo electrónico y navegador web: Proteja y gestione los navegadores web y los sistemas de correo electrónico contra las amenazas basadas en la web para minimizar su superficie de ataque. Deshabilite los navegadores no autorizados y los plug-ins de los clientes de correo electrónico, y garantice que los usuarios puedan acceder sólo a sitios web de confianza manteniendo filtros de URL basados en la red.

Control 8: Defensas contra malware: Controle la instalación y ejecución de código malicioso en varios puntos de su empresa para prevenir los ataques. Configure e implemente software antimalware y optimice el uso de la automatización para permitir una rápida actualización de las defensas y una rápida acción correctiva cuando se producen los ataques.

Control 9: Limitación y control de puertos de red, protocolos y servicios: Supervise y controle la actividad en los puertos, protocolos y servicios de los dispositivos de la red para reducir el alcance de los ataques mediante las vulnerabilidades del servicio. Aproveche los firewalls del host para garantizar que sólo se permita el acceso al tráfico apropiado.

Control 10: Funciones de recuperación de datos: Establezca procesos y herramientas para garantizar que la información crítica de su organización esté debidamente respaldada, y disponga de un sistema de recuperación de datos fiable para la restauración de los

datos a fin de superar los ataques que ponen en peligro los datos críticos.

Control 11: Configuración segura para dispositivos de red, tales como firewalls, routers y switches: Establezca, implemente y gestione la configuración de seguridad de los dispositivos de red para evitar que los atacantes se aprovechen de las configuraciones predeterminadas vulnerables. Disponga de un proceso estricto de gestión y control de configuraciones para garantizar que éstas no se encuentren en un estado explotable.

Control 12: Protección perimetral: Detecte, prevenga y controle el flujo de información a través de los perímetros de su red para evitar que los atacantes obtengan acceso pasando por alto los sistemas perimetrales. Configure el monitoreo perimetral, deniegue el acceso no autorizado e implemente sistemas de detección de intrusos para reforzar la protección perimetral.

Control 13: Protección de datos: Identifique y segregue los datos sensibles e implemente una combinación de procesos, incluidos la codificación, los planes de protección contra la infiltración de datos y las técnicas de prevención de pérdida de datos, para garantizar la privacidad e integridad de los datos sensibles.

Control 14: Control de acceso basado en la necesidad de saber: Supervise, controle y proteja el acceso a los activos críticos, como la información, los recursos y los sistemas. Permita el acceso a información crítica sobre la base de la necesidad de saberla y establezca un registro detallado de los servidores a fin de supervisar el acceso e investigar los incidentes en los que se haya accedido indebidamente a los datos.

Control 15: Control de acceso inalámbrico: Supervise, controle y proteja sus redes de área local inalámbricas (WLAN), puntos de acceso y sistemas de clientes inalámbricos para evitar que los atacantes manipulen sus defensas perimetrales. Implemente un sistema de detección de intrusos inalámbricos y lleve a cabo un análisis de vulnerabilidades en los equipos de clientes inalámbricos para detectar vulnerabilidades explotables.

Control 16: Monitoreo y control de cuentas: Gestione activamente todo el ciclo de vida de sus sistemas y cuentas de aplicaciones, desde su creación, uso e inactividad hasta su eliminación, para evitar que los atacantes exploten las cuentas de usuarios legítimos pero inactivos.

Control 17: Implementar un programa de concienciación y capacitación en seguridad: Implemente un plan integrado para identificar, desarrollar e instruir a los empleados sobre las habilidades y destrezas específicas que deben poseer para apoyar la defensa de la empresa de acuerdo con su rol funcional en la organización.

Control 18: Seguridad del software de aplicación: Ponga a prueba regularmente todo su software desarrollado internamente y adquirido para detectar vulnerabilidades. Disponga de un programa eficaz para abordar la seguridad a lo largo de todo el ciclo de vida del software interno, incluidos el establecimiento de los requisitos, la capacitación, las herramientas y las pruebas, y disponga de criterios estrictos de evaluación de la seguridad al adquirir software de terceros.

Control 19: Respuesta y gestión de incidentes: Desarrolle e implemente un sistema de gestión de incidentes definido en su organización para descubrir rápidamente los ataques, contener eficazmente los daños, erradicar la presencia del atacante y restablecer las operaciones con rapidez.

Control 20: Pruebas de penetración y ejercicios de equipo rojo: Ponga a prueba periódicamente sus defensas para identificar las brechas y evaluar la preparación de su organización frente a los ataques mediante la realización de pruebas de penetración. Simule los objetivos y acciones de un atacante con la ayuda de equipos rojos para inspeccionar su actual postura de seguridad y así obtener valiosos conocimientos sobre la eficacia de sus defensas.

COBIT 5

¿Qué es?

Por sus siglas en ingles Control Objectives for Information and Related Technologies es un marco de trabajo de larga data creado por ISACA hace casi 25 años. El marco cubre todos los procesos más importantes necesarios para una gestión eficaz de las TI. La versión más reciente, COBIT 5, hace mucho hincapié en la seguridad de la información, sobre todo a la hora de abordar el cambiante permiso empresarial a raíz de factores como bring your own device y el trabajo remoto.

¿Cómo se implementa?

Este marco de trabajo cuenta con cinco principios que una organización debe seguir para adoptar la gestión de TI:

1. **Satisfacción de las necesidades de los accionistas:** se alinean las necesidades de los accionistas con los objetivos empresariales específicos, objetivos de TI y objetivos habilitadores. Se optimiza el uso de recursos cuando se obtienen beneficios con un nivel aceptable de riesgo.
2. **Considerar la empresa de punta a punta:** el gobierno de TI y la gestión de TI son asumidos desde una perspectiva global, de tal modo que se cubren todas las necesidades corporativas de TI. Esto se aplica desde una perspectiva "de punta a punta" basada en los 7 habilitadores de COBIT.
3. **Aplicar un único modelo de referencia integrado:** COBIT 5 integra los mejores marcos de Information Systems Audit and Control Association (ISACA) como Val IT, que relaciona los procesos de COBIT con los de la gerencia requeridos para conseguir un buen valor de las inversiones en TI. También se relaciona con Risk IT, lanzado por ISACA para ayudar a organizaciones a equilibrar los riesgos con los beneficios.
4. **Posibilitar un enfoque holístico:** los habilitadores de COBIT 5 están identificados en siete categorías que abarcan la empresa de punta a punta. Individual y colectivamente, estos factores influyen para que el gobierno de TI y la gestión de TI operen en función de las necesidades del negocio.
5. **Separar el gobierno de la gestión:** COBIT 5 distingue con claridad los ámbitos del gobierno de TI y la gestión de TI. Se entiende por gobierno de TI las funciones relacionadas con la evaluación, la dirección y el monitoreo de las TI. El gobierno busca asegurar el logro de los objetivos empresariales y también evalúa las necesidades de los accionistas, así como las condiciones y las opciones existentes. La dirección se concreta mediante la priorización y la toma efectiva de decisiones. Y el monitoreo abarca el desempeño, el cumplimiento y el progreso en función con los objetivos acordados. La gestión está más relacionada con la planificación, la construcción, la ejecución y el monitoreo de las actividades alineadas con la dirección establecida por el organismo de gobierno para el logro de los objetivos empresariales.

ISO/IEC 27001/27002

¿Qué es?

ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002.

Contar con esa certificación implica que una empresa está cumpliendo con las buenas prácticas implantadas en el Sistema de Gestión de Seguridad de la Información. Es decir, que cumplan con un régimen de legalidad para preservar su identidad, integridad y la confidencialidad de la información que emplean. Además, propone una serie de ventajas muy atractivas para las empresas, como mostrar una imagen empresarial más profesional y de confianza, mostrar un compromiso con la legalidad y la adecuación de sus recursos y ponerse en una significante ventaja competitiva dentro del mercado internacional.

¿Cómo se implementa?

ISO 27001

Definir los objetivos y redactar una Política de Seguridad: es importante tener los objetivos definidos y saber qué expectativas debe cumplir en todo momento la empresa para obtener dicha certificación. Tras definir la Política de Seguridad, esta deberá pasarse a la dirección para que pueda ser aprobada y estudie los recursos humanos y materiales necesarios para llevar a cabo su implementación.

Definir los riesgos: una vez tenemos ya pensada una Política de Seguridad, el siguiente paso que debemos dar será identificar los riesgos a los que se puede enfrentar la empresa, quién se encargará de gestionarlos, cuáles son las vulnerabilidades de la compañía.

Evaluar y analizar los riesgos: una vez se han identificado los riesgos a los que se expone la empresa, se debe analizar el impacto que podrían generar dichas amenazas sobre la compañía y con cuánta frecuencia podrían producirse. se debe realizar un tratamiento de riesgos, es decir, ver qué riesgos se pueden reducir y eliminar. De la misma forma, debemos buscar cuáles serán los métodos para gestionar dichos riesgos en caso de que ocurran.

Realizar la declaración de la aplicabilidad: una vez ya se ha realizado el tratamiento de riesgos, se deben definir los objetivos de control, ver cuáles se pueden aplicar y cuáles no, cómo se hará y por qué se hará. Todo esto deberá quedar

recogido en un documento llamado "Declaración de Aplicabilidad".

Poner en marcha la implementación del Sistema de Gestión de Seguridad de la Información: Una vez que se ha pasado la fase de planificación, es el momento de implementar el SGSI, y, por tanto, el plan de tratamiento del riesgo previsto. Se deberán introducir nuevas tecnologías y prácticas que ayuden a alcanzar los objetivos marcados y realizar controles de seguridad.

Capacitación y concienciación: una empresa no es nada sin las personas que la conforman. La puesta en marcha no se podrá llevar a cabo correctamente si no se forma a los empleados para que puedan actuar siguiendo las nuevas medidas impuestas. En este paso, es primordial la formación del personal en cuanto a las nuevas tecnologías aplicadas y los nuevos protocolos que se hayan establecido.

Monitoreo: Es importante que, antes de obtener la certificación, nos aseguremos de la efectividad de los procesos que se han implementado en la compañía. Por ello, se debe dedicar un periodo de tiempo a medir, controlar y revisar cómo funciona el sistema y si está permitiendo que se alcancen los objetivos establecidos.

ISO 27002

Sección 5 – Política de Seguridad de la Información: Se debe crear un documento sobre la política de seguridad de la información de la empresa, que debe contener los conceptos de seguridad de la información, una estructura para establecer los objetivos y las formas de control, el compromiso de la dirección con la política, entre tantos otros factores.

Sección 6 – Organización de la Seguridad de la Información: Para implementar la Seguridad de la Información en una empresa, es necesario establecer una estructura para gestionarla de una manera adecuada. Para ello, las actividades de seguridad de la información deben ser coordinadas por representantes de la organización, que deben tener responsabilidades bien definidas y proteger las informaciones de carácter confidencial.

Sección 7 – Gestión de activos: Activo, según la norma, es cualquier cosa que tenga valor para la organización y que necesita ser protegido. Pero para ello los activos deben ser

identificados y clasificados, de modo que un inventario pueda ser estructurado y posteriormente mantenido. Además, deben seguir reglas documentadas, que definen qué tipo de uso se permite hacer con dichos activos.

Sección 8 – Seguridad en recursos humanos: Antes de la contratación de un empleado o incluso de proveedores es importante que sea debidamente analizado, principalmente si se trata de información de carácter confidencial. La intención de esta sección es mitigar el riesgo de robo, fraude o mal uso de los recursos. Y cuando el empleado esté trabajando en la empresa, debe ser consciente de las amenazas relativas a la seguridad de la información, así como de sus responsabilidades y obligaciones.

Sección 9 – Seguridad física y del medio ambiente: Los equipos e instalaciones de procesamiento de información crítica o sensible deben mantenerse en áreas seguras, con niveles y controles de acceso apropiados, incluyendo protección contra amenazas físicas y ambientales.

Sección 10 – Seguridad de las operaciones y comunicaciones: Es importante que estén definidos los procedimientos y responsabilidades por la gestión y operación de todos los recursos de procesamiento de la información. Esto incluye la gestión de servicios tercerizados, la planificación de recursos de los sistemas para minimizar el riesgo de fallas, la creación de procedimientos para la generación de copias de seguridad y su recuperación, así como la administración segura de las redes de comunicaciones.

Sección 11 – Control de acceso: El acceso a la información, así como a los recursos de procesamiento de la información y los procesos de negocios, debe ser controlado con base en los requisitos de negocio y en la seguridad de la información. Debe garantizarse el acceso de usuario autorizado y prevenido el acceso no autorizado a los sistemas de información, a fin de evitar daños a documentos y recursos de procesamiento de la información que estén al alcance de cualquiera.

Sección 12 – Adquisición, desarrollo y mantenimiento de sistemas: Los requisitos de seguridad de los sistemas de información deben ser identificados y acordados antes de su desarrollo y/o de su implementación, para que así puedan ser protegidos para el mantenimiento de su confidencialidad, autenticidad o integridad por medios criptográficos.

Sección 13 – Gestión de incidentes de seguridad de la información: Los procedimientos formales de registro y escalonamiento deben ser establecidos y los empleados, proveedores y terceros deben ser conscientes de los procedimientos para notificar los eventos de seguridad de la información para asegurar que se comuniquen lo más rápido posible y corregidos en tiempo hábil.

Sección 14 – Gestión de continuidad del negocio: Los planes de continuidad del negocio deben ser desarrollados e implementados, con el fin de impedir la interrupción de las actividades del negocio y asegurar que las operaciones esenciales sean rápidamente recuperadas.

Sección 15 – Conformidad: Es importante evitar la violación de cualquier ley criminal o civil, garantizando estatutos, regulaciones u obligaciones contractuales y de cualesquiera requisitos de seguridad de la información. En caso necesario, la empresa puede contratar una consultoría especializada, para que se verifique su conformidad y adherencia a los requisitos legales y reglamentarios.

ITIL 4

¿Qué es?

ITIL 4 es una revisión al marco de trabajo más ampliamente aceptado a nivel mundial para la Administración de Servicios de TI (ITSM). Se compone de una guía comprensiva de como adoptar y adaptar las mejores prácticas de gestión.

ITIL 4 proporciona la guía que necesitan las organizaciones para abordar los nuevos desafíos de la administración de servicios y utilizar el potencial de la tecnología moderna. Está diseñado para garantizar un sistema flexible, coordinado e integrado para el gobierno y la gestión efectiva de los servicios habilitados para TI.

¿Cómo se implementa?

1. Primeros pasos: es muy importante que las figuras clave de la gestión conozcan los principios de ITIL y se comprometan con la implementación de ITIL. Eso ayudará a garantizar la atención adecuada de la gerencia y asegurar el financiamiento, la capacitación y otros recursos necesarios para una implementación exitosa.

También es importante establecer la persona o el rol responsable de la gestión de procesos de ITIL, quien se asegurará de que todos los procesos funcionen en conjunto, que se proporcionen las herramientas necesarias y que los procesos estén bien documentados.

2. Definición del servicio: Hay que crear una descripción general del servicio, compuesta por servicios comerciales y servicios de TI que los respaldan (servicios de soporte). Los servicios empresariales son los que representan valor directo para la empresa (clientes), y los servicios de apoyo son los que no hacen eso, pero son necesarios para ejecutar los servicios empresariales.

3. Introducción de roles y propietarios de ITIL: Es muy importante saber, en cualquier momento, quién es responsable de qué y, por lo tanto, introducir roles y funciones designados de acuerdo con el marco ITIL. Según el alcance de la implementación de ITIL, es posible que no se requieran todos los roles de ITIL en su caso, pero es imprescindible identificar los roles y propietarios clave. Los roles y su participación dentro del ciclo de vida del servicio se mantienen en una matriz RACI (Responsable, Responsable, Consultado, Informado).

4. Análisis de brechas: Un análisis de brechas es básicamente un informe sobre qué procesos necesita cambiar, cuáles debe abandonar y dónde deben introducirse otros nuevos. Un análisis de brechas podría centrarse en la tecnología de la información en general o en algún aspecto de la tecnología de la información, como la implementación de una herramienta. Al final, las conclusiones de un análisis de brechas deben describir cuánto esfuerzo se requiere en términos de tiempo, dinero y recursos humanos para lograr la visión.

5. Planificación de nuevos procesos: es importante considerar las mejores prácticas de ITIL en su conjunto; esto significa que, si está implementando la gestión de incidentes, también debe considerar la implementación de la gestión de problemas, debido a la estrecha relación entre los dos.

6. Control de procesos: Al diseñar un proceso, es importante implementar métricas medibles (KPI) que muestren claramente si el proceso se ejecuta de acuerdo con las expectativas o no, porque esa información es muy importante para los propietarios del proceso.

7. Hoja de ruta de implementación: El propósito de una hoja de ruta de implementación es proporcionar una descripción general de todos los pasos necesarios para completar con éxito el proyecto.

8. Implementación de procesos ITIL: Se debe verificar si el plan de implementación cumplió con las expectativas, si todos los servicios se implementaron con éxito y si sus procesos están produciendo los resultados que deseaba.

NIST CSF

¿Qué es?

El Instituto Nacional de Estándares y Tecnología mejor conocido por sus siglas en inglés NIST, es un marco que se utiliza para la mejora de la seguridad cibernética en infraestructuras críticas. Tiene como propósito comprender, gestionar y reducir los riesgos cibernéticos. Proteger sus redes y datos.

Las cinco funciones del marco de ciberseguridad son:

Identificar: Ayuda a desarrollar un entendimiento organizacional para administrar el riesgo de ciberseguridad de los sistemas, las personas, los activos, los datos y las capacidades. La comprensión del contexto empresarial, los recursos que respaldan las funciones críticas y los riesgos relacionados con la ciberseguridad permiten que una organización se centre y priorice sus esfuerzos, de acuerdo con su estrategia de administración de riesgos y sus necesidades comerciales.

Proteger: Describe las medidas de seguridad adecuadas para garantizar la entrega de servicios de las infraestructuras críticas. Esta función contempla la capacidad de limitar o contener el impacto de un potencial evento de ciberseguridad.

Detectar: Define las actividades necesarias para identificar la ocurrencia de un evento de ciberseguridad, permitiendo el descubrimiento oportuno de los mismos.

Responder: Incluye actividades necesarias para tomar medidas con respecto a un incidente de ciberseguridad detectado, desarrollando la capacidad de contener el impacto de un potencial incidente desarrollando la capacidad de contener el impacto de un potencial incidente.

Recuperar: Identifica las actividades necesarias para mantener los planes de resiliencia y para restaurar cualquier capacidad o servicio que se haya deteriorado debido a un incidente de ciberseguridad. Esta función es compatible con la recuperación oportuna de las operaciones normales para reducir el impacto de un incidente de ciberseguridad.

¿Cómo se implementa?

TIER 1:

Parcial: Proceso de gestión de riesgos: Las prácticas de gestión de riesgos de ciberseguridad de la organización no están formalizadas, y el riesgo se gestiona de forma ad hoc y, en ocasiones, de forma reactiva. La priorización de las actividades de ciberseguridad puede no estar directamente informada por los objetivos de riesgo de la organización, el entorno de amenaza o los requisitos de negocios / misión.

Programa integrado de gestión de riesgos: Existe una conciencia limitada sobre el riesgo de seguridad cibernética a nivel organizacional y no se ha establecido un enfoque de toda la organización para gestionar el riesgo de ciberseguridad. La organización implementa la gestión del riesgo de ciberseguridad en forma irregular caso por caso debido a la experiencia variada o la información obtenida de fuentes externas. La organización puede no tener procesos que permitan compartir información de ciberseguridad dentro de la organización.

Participación externa: La organización puede no tener los procesos establecidos para participar en la coordinación o colaboración con otras entidades.

TIER 2: Riesgos de información

Proceso de gestión de riesgos: Las prácticas de gestión de riesgos son aprobadas por la administración, pero no pueden establecerse como políticas de toda la organización. La priorización de las actividades de ciberseguridad está directamente relacionada con los objetivos de riesgo de la organización, el entorno de amenazas o los requisitos de negocios / misiones.

Programa integrado de gestión de riesgos: Existe una conciencia del riesgo de ciberseguridad a nivel organizacional, pero no se ha establecido un enfoque de toda la organización para gestionar el riesgo de ciberseguridad. Los procesos y procedimientos

informados por el riesgo, aprobados por la gerencia, se definen e implementan, y el personal cuenta con los recursos adecuados para realizar sus tareas de ciberseguridad. La información de ciberseguridad se comparte dentro de la organización de manera informal.

Participación externa: La organización conoce su rol en el ecosistema más grande, pero no ha formalizado sus capacidades para interactuar y compartir información externamente.

TIER 3: Repetible

Proceso de gestión de riesgos: Las prácticas de gestión de riesgos de la organización se aprueban formalmente y se expresan como políticas. Las prácticas de ciberseguridad organizacional se actualizan periódicamente en función de la aplicación de los procesos de gestión de riesgos a los cambios en los requisitos empresariales / de la misión y un panorama cambiante de amenazas y tecnología.

Programa integrado de gestión de riesgos: Existe un enfoque de toda la organización para gestionar el riesgo de ciberseguridad. Las políticas, procesos y procedimientos informados sobre riesgos se definen, implementan según lo previsto y se revisan. Se han implementado métodos consistentes para responder de manera efectiva a los cambios en el riesgo. El personal posee el conocimiento y las habilidades para realizar sus roles y responsabilidades asignados.

Participación externa: La organización entiende sus dependencias y socios y recibe información de estos socios que permite la colaboración y las decisiones de gestión basadas en riesgos dentro de la organización en respuesta a los eventos.

TIER 3: Adaptable

Proceso de gestión de riesgos: La organización adapta sus prácticas de ciberseguridad en función de las lecciones aprendidas y los indicadores predictivos derivados de las actividades de ciberseguridad anteriores y actuales. A través de un proceso de mejora continua que incorpora prácticas y tecnologías avanzadas de ciberseguridad, la organización se adapta activamente a un entorno cambiante de ciberseguridad y responde a las amenazas cambiantes y sofisticadas de manera oportuna.

Programa integrado de gestión de riesgos: Existe un enfoque de toda la organización para gestionar el riesgo de ciberseguridad que utiliza políticas, procesos y procedimientos informados sobre riesgos para abordar posibles eventos de ciberseguridad. La gestión del

riesgo de ciberseguridad forma parte de la cultura organizacional y evoluciona a partir de la conciencia de las actividades previas, la información compartida por otras fuentes y el conocimiento continuo de las actividades en sus sistemas y redes.

Participación externa: La organización gestiona los riesgos y comparte activamente la información con los socios para garantizar que la información precisa y actualizada se distribuya y consuma para mejorar la ciberseguridad antes de que se produzca un evento de seguridad.

NIST SP 800-53

¿Qué es?

Es un marco continuamente actualizado que trata de definir de manera flexible estándares, controles y evaluaciones en función del riesgo, la rentabilidad y las capacidades.

Tiene como propósito proporcionar una base de elementos guía, estrategias, sistemas y controles, que pueden respaldar de forma independiente las necesidades y prioridades de ciberseguridad de cualquier organización.

¿Cómo se implementa?

CA - Control de acceso: La familia de control de CA consta de requisitos de seguridad que detallan el registro del sistema. Esto incluye quién tiene acceso a qué activos y capacidades de generación de informes, como administración de cuentas, privilegios del sistema y registro de acceso remoto para determinar cuándo los usuarios tienen acceso al sistema y su nivel de acceso.

AU - Auditoría y rendición de cuentas: La familia de controles AU consta de controles de seguridad relacionados con las capacidades de auditoría de una organización. Esto incluye políticas y procedimientos de auditoría, registro de auditoría, generación de informes de auditoría y protección de la información de auditoría.

AT - Sensibilización y Formación: Los conjuntos de control de la familia de controles AT son específicos para su capacitación y procedimientos de seguridad, incluidos los registros de capacitación de seguridad.

CM - Gestión de la configuración: Los controles de CM son específicos de las políticas de gestión de la configuración de una organización. Esto incluye una configuración básica para operar como base para futuras construcciones o cambios en los sistemas de

información. Adicionalmente, esto incluye inventarios de componentes del sistema de información y un control de análisis de impacto de seguridad.

CP - Planificación de Contingencias: La familia de controles CP incluye controles específicos para el plan de contingencia de una organización en caso de que ocurra un evento de ciberseguridad. Esto incluye controles como pruebas, actualizaciones, capacitación y copias de seguridad del plan de contingencia, y reconstitución del sistema.

IA - Identificación y Autenticación: Los controles de IA son específicos de las políticas de identificación y autenticación en una organización. Esto incluye la identificación y autenticación de usuarios organizacionales y no organizacionales y cómo la gestión de esos sistemas.

Se puede asegurar que se cumple con este marco de ciberseguridad con los siguientes pasos:

PASO 1: Delegar responsabilidad

PASO 2: Comprender las políticas y operaciones existentes

PASO 3: Adoptar un enfoque común para la implementación cuando sea posible

PASO 4: Referencia al catálogo de control.

PASO 5: Registrar evidencia de implementación

PCI SSC

¿Qué es?

Payment Card Industry Data Security Standard por sus siglas en inglés, es un foro compuesto por cinco de las más importantes marcas de pago: Visa Inc., MasterCard, American Express, Discover Financial Services y JCB International. Se creo con el objetivo de definir los controles de seguridad orientados hacia la protección de los datos de tarjetas de pago durante todo el flujo transaccional.

¿Cómo se implementa?

Construya y mantenga redes y sistemas protegidos

1. Instale y mantenga controles de seguridad en las redes.
2. Aplique configuraciones protegidas para todos los componentes del sistema.

Proteja los datos del titular de la tarjeta

1. Proteja los datos de cuenta almacenados.
2. Proteja los datos del titular de la tarjeta con una sólida criptografía durante la transmisión a través de redes públicas abiertas

Mantenga un programa de gestión de vulnerabilidades:

1. Proteja todos los sistemas y redes de software malintencionado.
2. Desarrolle y mantenga sistemas y softwares protegidos.

Implemente medidas solidas de control de acceso

1. Restrinja el acceso a los componentes del sistema y a los datos del titular de la tarjeta según las necesidades comerciales.
2. Identifique a los usuarios y autentique a los componentes del sistema.
3. Restrinja el acceso físico a datos del titular de la tarjeta.

Monitorear y verificar las redes regularmente

1. Registre y monitoree todo el acceso a los componentes del sistema y a los datos del titular de la tarjeta.
2. Verifique la seguridad de los sistemas y redes regularmente.

Mantenga una política de protección informática

3. Respalde la protección informática con políticas y programas organizacionales.

RECOMENDACIONES

Series/ Películas/ Documentales

Nada es privado

https://www.youtube.com/watch?v=HVHKYXJq7qo

El dilema de las redes sociales

https://www.youtube.com/watch?v=EBxHl0H7Y0g

Clickbait

https://www.youtube.com/watch?v=JZJo0BFZDQ8

We Steal Secrets: The Story of WikiLeaks

https://www.youtube.com/watch?v=WUjA_hcYzzI

The Secret History of Hacking

Podcast

Pegasus: sonríe te estamos grabandoLinks to an external site.

https://elhilo.audio/podcast/pegasus-mx/

Profiling People with Social Media

https://www.social-engineer.org/podcasts/episode-031-profiling-people-with-social-media/

You Are Special And Other Lies With Cortney Warren

https://www.social-engineer.org/podcasts/ep-153-human-element-series-you-are-special-and-other-lies-with-cortney-warren/

CONCLUSIONES

1. Existen diferentes marcos de ciberseguridad que se adaptan a las empresas dependiendo de sus necesidades.
2. Saber sobre ciberseguridad debería ser parte de la cultura general, ya que la tecnología es algo que nos acompaña día a día.
3. La ciberseguridad tiene relación con varias especialidades, como por ejemplo la psicología, que nos hace reflexionar mejor la manera en que somos vulnerables.
4. Se pueden implementar varios marcos de ciberseguridad en una empresa.

REFERENCIAS

[1] CIS (2022). CIS Controls V8. Extraido de: https://www.cisecurity.org/controls/v8

[2] Cisco Systems (2022). What is cybersecurity? Extraído de: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html#~temas-relacionados

[3] IBM (2022). Cybersecurity. Extraído de: https://www.ibm.com/es-es/topics/cybersecurity

[4] ISACA (2022). COBIT. Extraído de: https://www.isaca.org/resources/cobit

[5] ISO (2022). ISO 27001. Extraído de: https://www.iso.org/isoiec-27001-information-security.html

[6] ISO (2022). ISO 27002. Extraído de: https://www.iso.org/standard/75652.html

[7] Kaspersky (2022). What is cyber security? Extraído de: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

[8] Microsoft (2022). ¿Qué es la ciberseguridad? Extraído de: https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-la-ciberseguridad-8b6efd59-41ff-4743-87c8-0850a352a390

[9] Nist (2022) Cybersecurity Framework. Extraído de: https://www.nist.gov/cyberframework

[10] Nist (2022) SP 800-53. Extraído de: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[11] PCI SSD (2022). PCI Security Standar https://www.pcisecuritystandards.org/