APUNTES 02

DISEÑO DE PLANES DE SECURIZACIÓN

BASTIONADO DE REDES Y SISTEMAS

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

ÍNDICE

En esta unidad de trabajo estudiarás los conceptos básicos sobre el desarrollo de planes de seguridad asociados a las tareas de bastionado de redes y sistemas. Comenzando por un análisis de riesgos hasta la implementación de un plan director de seguridad. Para ellos se darán a conocer cuáles son las medidas técnicas, las políticas de seguridad más usadas así como las guías de buenas prácticas más populares sin dejar de lado la caracterización de procesos.
Además también conocerá los principios de la economía circular y su importancia en la actualidad.

1.- ANÁLISIS DE RIESGOS

Esta fase conlleva una serie de actividades que describiremos a continuación.
1.- Conocer la situación actual del sistema/organización
Sin duda es indispensable conocer la situación actual en términos de ciberseguridad de la organización o sistema sobre el que vamos a hacer el análisis. Nunca podremos estar seguros de si realmente estamos elevando el nivel de seguridad si no conocemos la situación de partida.
Para llevar a cabo este primer análisis, tendremos en cuenta los aspectos esenciales sobre los que hemos de realizarlo como por ejemplo:

- Nivel de madurez de la empresa
- Elementos técnicos
- Aspectos organizativos
- Cumplimiento o normativa vigente
- Criticidad de la información

Como se puede inferir, este primer análisis, es necesario implicar a toda la organización, pues debemos realizar una serie de actividades como entrevistas, cuestionarios, etc. para recopilar la información necesaria de cara a llevar a cabo el análisis. En este punto podríamos encontrar dificultades o problemas como que no se nos facilitara toda la información, de manera intencionada o no, no contar con el apoyo de áreas críticas, como el área de TI, etc. Además será necesario contar con el apoyo de la dirección o la parte estratégica de la organización para esta cuestión ya que, por ejemplo, si no creen en las bondades de la ciberseguridad, difícilmente podremos incrementar el nivel de seguridad ya que no se facilitará presupuesto y se demorarán los plazos establecidos priorizando otras cuestiones.

2.- Limitar el alcance
Para poder implementar ciberseguridad desde un punto de vista efectivo y eficiente, se ha de limitar el alcance del proyecto y este además ha de ser realista. Por un lado para conocer el tamaño de las tareas que tendremos que llevar a cabo, y por otro para concretar sobre qué áreas o procesos se llevará a cabo. Por ejemplo, en una empresa dedicada a la investigación, una de las áreas más importantes a proteger será la relativa a I+D+i.

Atendiendo a lo anterior, tendremos que realizar una identificación de activos que serán los objetivos donde se aplicarán los controles de seguridad que implementemos, tanto a nivel técnico como organizativo sin olvidar los de carácter normativo. Lo habitual es que una vez determinados los más críticos, las tareas de protección comiencen por estos. Un buen punto de partida para determinar qué controles se han de implementar, podría estar basado en el listado de la norma ISO/IEC 27001 introducida en la unidad 1. Estos controles han de estar dirigidos por los que se denominan escalas o modelos de madurez que pueden tener distintos valores en función de cómo se encuentre implementado en la organización.
Tomando como ejemplo los basados en CMM y considerando el control relativo a las copias de seguridad, este podría ser:

- Inexistente: carecen de política de copias de seguridad.
- Inicial: disponen de un sistema, pero nadie las controla ni se planifican.
- Repetible: se lleva a cabo la política pero sin ningún tipo de normalización, habitualmente bajo demanda.
- Definido: existe un procedimiento claro, pero no está aprobado por la dirección.
- Administrado: existe un procedimiento formal que ha sido aprobado.
- Optimizado: existe un procedimiento formal que ha sido aprobado y se verifica su eficacia periódicamente mediante indicadores.

1.1.- FASES DEL ANÁLISIS. INTEF (CC BY-NC-SA)

Paralelamente a las cuestiones previas, llevaremos a cabo el análisis propiamente dicho en todas sus fases para obtener el listado de posibles amenazas que podrían afectar al sistema analizado. En la unidad uno ya introducimos las diferentes metodologías y estándares existentes para llevar a cabo esta tarea y estas presentan aspectos comunes. Sin duda el que confluye en todas, es el valorar cada activo para establecer posteriormente la priorización.Entre las fases para llevar a cabo esta tarea destacamos:

Fase inicial: reconocimiento

1. Identificación de activos: identificar las amenazas a las que podrían estar sujetos.
2. Identificación del riesgo intrínseco: resultante de la fase previa y que, nos dará el nivel de riesgo del activo sin la aplicación de los controles que mejorarán la seguridad.
3. Probabilidad de ocurrencia: estableceremos la posibilidad de que se materialice la amenaza sobre el activo y que pueda generar un impacto y las consecuencias derivadas. En este punto podremos calcular el nivel de riesgo siguiendo la fórmula: Riesgo= Impacto (€) x probabilidad. En este sentido y usando un ejemplo, si para nuestra empresa, la falta de acceso a la información de los servidores físicos a causa de un incendio en las instalaciones podría costarnos 1000€ al día y eso se puede prorrogar durante un mes, y considerando una probabilidad baja en una escala del 1 al 10, la fórmula podría quedar de la siguiente manera: Riesgo=(1000x30)x2, resultando una cantidad de 60000€ en posibles pérdidas. Esto evidentemente indica que se requiere establecer un control para esta cuestión.
4. Riesgos no aceptables: tras el paso previo, hemos de identificar aquellos riesgos que no son aceptables. Estos serían aquellos que pueden afectar muy negativamente al negocio hasta el punto de dejar la organización sin servicio. El tipo de control a implementar, será siempre proporcional al activo que se quiere proteger.
5. Riesgo residual: determinará el nivel de riesgo tras su reducción considerando este con un valor “aceptable”.

Mitigación de los riesgos

Tras la fase previa, en esta será donde se establecerán los mecanismos y controles que permitirán definir un nivel de riesgo aceptable y asumible. ¿Con qué mecanismos contamos para llevar a cabo esta tarea? Podemos implementar los siguientes:

1. Implementar controles para su mitigación: suele ser la más habitual cuando se trata de problemas que pueden interferir en el correcto funcionamiento de los procesos de una organización.
2. Eliminando el riesgo: cuando se trata de un proceso que no es necesario pero que podría poner en peligro otros activos de la organización.
3. Tercerizar o transferir el riesgo: a través por ejemplo de un ciberseguro o una póliza de ciberriesgos.

Establecimiento de indicadores y verificación del proceso

Tras definir los controles, se han de establecer cuadros de mando que nos permitan medir el correcto funcionamiento de los controles. Si no tenemos en cuenta esta cuestión, es decir si no medimos, nunca sabremos si realmente el control está funcionando. Por ejemplo, en una política de copias de seguridad, si no comprobamos la frecuencia con que se hacen y si no verificamos su posible restauración, no podremos estar seguros de si realmente la misma está funcionando de manera correcta. De esta manera verificaremos que la medida que se ha implementado es efectiva contra el riesgo que queremos reducir.

Por último, es importante indicar, que el análisis de riesgos es un proceso continuo y que se debe llevar a cabo de manera periódica pues las tecnologías, servicios e infraestructuras de las organizaciones cambian frecuentemente en el mundo TI. Se trata como indicamos en la unidad 1, de un proceso de mejora continua.

2.- PRINCIPIOS DE LA ECONOMÍA CIRCULAR

Caso práctico

Es importante disponer de sistemas productivos que permitan el reciclaje y la sostenibilidad. Por ejemplo, aquellas organizaciones que producen con materias tipo monocomponente, en el futuro serán sostenibles.

El proceso productivo actual, no es sostenible. Se trata de un proceso lineal donde se usa demasiada materia prima que luego no es posible reciclar o reutilizar, o al menos en un porcentaje que garantice unos niveles de sostenibilidad adecuados.

La economía circular en la industria 4.0, es básicamente en un sistema que permita aprovechar los recursos, reduciendo elementos innecesarios que por su naturaleza no pueden volver al medio ambiente.

Algunos de sus principios fundamentales (Fuente Corponet):

- El residuo se convierte en recurso. Todo el material biodegradable vuelve a la naturaleza y el no biodegradable se reutiliza.
- Reintroducir en el circuito económico aquellos productos que ya no corresponden a las necesidades iniciales de los consumidores.
- Reutilizar ciertos residuos o partes de ellos que todavía pueden funcionar para elaborar nuevos productos.
- Reparar y encontrar una segunda vida para los productos estropeados o defectuosos. Reciclar los materiales que se encuentran en los residuos.
- Aprovechar energéticamente los residuos que no se pueden reciclar.
- Eliminar la venta de ciertos productos para implantar un sistema de alquiler de bienes.
- Cuando el producto cumple su función principal, vuelve a la empresa y esta lo desmonta para reutilizar las piezas que pueden ser utilizadas nuevamente.
- Eliminar los combustibles fósiles para producir el producto, reutilizar y reciclar.
- Considerar los impactos medioambientales a lo largo del ciclo de vida de un producto y los integra desde su concepción.
- Establecer un método de organización industrial en un mismo territorio caracterizado por una gestión optimizada de los stocks y de los flujos de materiales, energía y servicios.

En el mundo TI por ejemplo, se busca poner fin a la obsolescencia programada y diseñar productos que sean sostenibles y eficaces en el tiempo, pero no sólo eso, si no que los avances tecnológicos como la inteligencia artificial, el Big Data y otras tecnologías, mejoras los procesos aunque no es ninguna panacea. En cualquier caso, aún estamos comenzando con este proceso y será esencial en los próximos años para garantizar la buena salud del medio ambiente.

Esta cita del Dr. Edmond Locard es conocida como el Principio de Locard, y del mismo se deduce que, a la hora de realizar el propio análisis forense, hay que ser especialmente cuidadoso para que el sistema se vea afectado en la menor medida posible y que las evidencias adquiridas no se vean alteradas, debido a que el uso de cualquier dispositivo informático siempre puede dejar algún tipo de rastro.

3.- MEDIDAS TÉCNICAS DE SEGURIDAD

Caso práctico

Para implementar seguridad, además del factor humano, hay que considerar las tecnologías. Imaginemos que una persona tiene que encargarse de comprobar uno a uno los archivos para ver si contienen virus o no. Sería una tarea titánica y que estaría sujeta a fallos debido al cansancio que provocaría. De este modo mediante una medida técnica como un antivirus, servirá para llevar a cabo dicha tarea de manera más eficiente y eficaz.

En este punto entraremos a describir diferentes medidas técnicas de seguridad adecuadas para reforzar la seguridad de los sistemas.

Es obvio que cuando hablamos de ciberseguridad, lo primero que nos suele venir a la cabeza, es lo relativo a tecnologías y herramientas. Evidentemente estas tienen gran importancia, pero no son lo único que hemos de tener en cuenta a la hora de bastionar una infraestructura.

Podemos definir como medida técnica de seguridad “aquella que ha sido diseñada en base a una tecnología o varias, cuyo propósito es proteger un activo o servicio de alguna amenaza o riesgo y que habitualmente ha de proteger las tres dimensiones de la seguridad de la información: la confidencialidad, la integridad y la disponibilidad”. En este sentido podemos contener dichas medidas en dos grupos fundamentales:

Medidas preventivas

Dentro de este grupo, enumeramos algunas de las principales herramientas o grupos de herramientas destinadas a evitar que se materialice una amenaza en un activo. Habitualmente siempre se suele decir que “es mejor prevenir que lamentar” y en el mundo de las TI podríamos suscribir dicha frase. Evidentemente si un día nos infectamos con un ransomware, nos acordaremos de que deberíamos haber instalado una aplicación antimalware. En esta ocasión describiremos algunos grupos de controles:

- Herramientas antimalware: se trata de la solución más básica. Los comúnmente conocidos como antivirus aunque desde hace unos años, disponen de otras funcionalidades integradas como cortafuegos.
- EDR y XDR: se trata de soluciones antimalware más modernas que las anteriores y que además disponen de medidas o funciones reactivas. EDR (Endpoint Detection and Response) se puede considerar la primera generación de este tipo de soluciones, y XDR (Extended Detection and Response) como la segunda. Ambas usan inteligencia artificial y otras técnicas para prever posibles ataques y patrones.
- Firewalls o cortafuegos: se trata de herramientas que van a poder configurarse para permitir o impedir el tráfico entre las redes en base a las reglas que se establezcan.
- Copias de seguridad: sin duda la estrella de las medidas preventivas y reina de los planes de contingencia. En caso de pérdida de la información, nos permitirá recuperarla.
- DLP: Data Loss Prevention, son un conjunto de herramientas que velan por que la información de una compañía no se filtre o se envíe sin disponer de autorización, lo que también se conoce como una fuga de datos. Estas herramientas permiten mantener el control de la información sin perder productividad.
- Verificación de integridad: mediante este tipo de soluciones, será posible controlar la integridad de los archivos que forman parte de un sistema o arquitectura. A través de la construcción de una base de datos, si se produce algún cambio como por ejemplo un binario, la herramienta generará una alerta. Habitualmente se usan funciones de hash.
- Conexiones seguras: algo esencial para proteger las comunicaciones, es mantener la confidencialidad de los datos que discurren por ellas. Existen numerosas herramientas pero destaca la implementación de VPNs (Virtual Private Networks) y otro tipo de soluciones de encapsulado. Si algún atacante intercepta el tráfico, en principio no podrá leerlo.
- IDS: los sistemas de detección de intrusos, son herramientas de carácter preventivo que informan ante un comportamiento anómalo en la red o en un host, para llevar a cabo algún tipo de acción.
- Virtual patching: se trata de un conjunto de soluciones diseñadas sobre todo para aquellos sistemas de producción que están soportados por sistemas obsoletos y que no es posible cambiar.
- SIEMs: los sistemas de identificación de eventos de seguridad, son sin duda una de las herramientas más populares de los últimos años que ayudará a identificar comportamientos anómalos tanto en una red como en un host.

Medidas reactivas

En este grupo se encuentran las herramientas que en caso de identificación o en el peor de los casos, se materialice un incidente, puedan llevar a cabo alguna acción que permita contenerlo, eliminarlo o corregir la situación. Algunas herramientas de carácter reactivo, también se encuentran en el grupo previo.
Quizás podamos considerar que si disponemos de un buen conjunto de medidas técnicas de carácter preventivo, no tenga demasiado sentido contar con medidas reactivas. Sin duda estaríamos ante un gran error de contexto ya que suelen complementarse. Algunas de estas herramientas pasarían por:

- EDR y XDR: la función reactiva de estas herramientas pasa por contener, bloquear o eliminar la amenaza detectada. Los sistemas de inferencia que usan son muy avanzados y efectivos.
- IPS: se trata de un IDS pero con capacidad reactiva, es decir, si identifica un evento no autorizado, además de avisar, llevará a cabo algún tipo de acción como un bloqueo.
- Plan de contingencia: más que de una herramienta, se trata de una política que recoge varias herramientas o soluciones que permitirán restaurar la actividad de una organización a través de un procedimiento específico. Suelen involucrar herramientas de copia de seguridad, de gestión de incidentes, etc.
- Verificación de integridad: esta herramienta, además de prevenir, puede llevar a cabo acciones como la restauración de un archivo en caso de modificación no autorizada o similar.
- Virtual patching: como con otras soluciones que también tienen un carácter preventivo, el virtual patching va a poder bloquear o parar ciertas amenazas que puedan afectar al activo que protege.

4.- POLÍTICAS DE SECURIZACIÓN

Caso práctico

Los análisis de riesgos son fundamentales para una empresa. Por ejemplo, una organización que no haya llevado a cabo la identificación de sus procesos más críticos, como por ejemplo aquella que se dedica al ecommerce y no vela por la seguridad de su portal web, tendrá severos problemas para mantener la actividad. En este caso y de manera mínima, tendrá que disponer de una política de copias de seguridad para los datos así como una política de actualizaciones.

Existen numerosas formas de agrupar las políticas en base a diversos criterios. La clasificación más común podemos decir que es la que distingue a la parte técnica y a la parte organizativa. Pero antes de entrar en ese aspecto, es importante conocer la diferencia entre una política y una buena práctica. A menudo se confunden o se asocian dichos conceptos a la misma cuestión, algo que es incorrecto.

- Buena práctica: recomendación que no es de obligado cumplimiento.
- Política: instrucción de obligado cumplimiento y que, en caso de no proceder como se indica, es posible amonestar o llevar algún tipo de acción sancionadora.

Las políticas son una herramienta que permitirá implementar ciberseguridad en los distintos procesos que forman parte del negocio de una organización. Podemos distinguir dos grupos:

- Organizativas: hacen referencia cuestiones relacionadas con el comportamiento que deben tener por ejemplo, los empleados ante determinadas cuestiones y que normalmente no pueden ser protegidas mediante medidas técnicas. Por ejemplo, “Está prohibido compartir contraseñas”, o “será obligatorio destruir la documentación en papel”.
- Técnicas, permiten implementar medidas que automatizan el control que se quiere implementar. Por ejemplo, la necesidad de cambiar la contraseña cada “x” meses, su complejidad y tamaño se puede configurar a través de una directiva en el servidor.

Habitualmente, las políticas son de aplicación sobre tres elementos, los procesos, las personas y las tecnologías. En función de a quién se dirija tendrán unas características concretas que servirán para el diseño de la propia política. Es importante también, considerar que deben estar equilibradas y alineadas por un lado con el negocio, y por otro con la usabilidad de los sistemas. No será nunca recomendable implementar políticas tan restrictivas que impidan que los procesos del negocio se desarrollen con normalidad, es decir, la ciberseguridad ha de apoyar al negocio y no al contrario.

A continuación se ofrecerá un listado de las políticas más comunes tanto a nivel organizativo como técnico.

Organizativas

- Continuidad del negocio: esta política permitirá implementar los controles necesarios para que en caso de desastre, se pueda recuperar la actividad del negocio lo más rápido posible de manera que las consecuencias no sean muy negativas.
- Cumplimiento legal: a día de hoy y al menos en el Espacio Europeo, las empresas con independencia de si son públicas o de ámbito privado, han de cumplir una serie de leyes que en caso contrario, acarrearían duras sanciones. Algunas destacadas son el RGPD o la LOPDGDD. Esta política se implementa para garantizar el cumplimiento.
- Relación con proveedores: a día de hoy, no se concibe la actividad de una empresa sin múltiples colaboradores. En ocasiones, la falta de controles entre las transacciones que se realizan, podrían provocar un incidente. Esta política vela por que se haga de manera correcta sin poner en riesgo a la empresa.
- Concienciación y formación: sin duda de las más importantes de cara a permitir que los empleados puedan elevar el nivel de ciberseguridad. Una política de este tipo garantizará la existencia de un “firewall humano” que será capaz de identificar los incidentes y eliminarlos o reportarlos.
- Uso del correo electrónico: a pesar de que se asocia el uso de una tecnología, como un cliente, es importante conocer cómo se debe hacer. Habitualmente esto se relaciona con el uso corporativo eliminando el derecho relativo al uso personal.
- Uso de dispositivos corporativos: similar a la anterior, esta política regula las directrices que un empleado ha de asumir cuando usa un equipo corporativo, sea un PC, portátil o dispositivo móvil.
- Uso de contraseñas: en este caso, el control se refiere a todo lo que no puede ser controlado por una directiva o política técnica. Tal y como adelantamos en el punto previo, se refiere a la no compartición de contraseñas, a no apuntarlas en post-it, etc.
- Protección del puesto de trabajo: también dirigida a los empleados para hacer un uso correcto del entorno. Por ejemplo el bloqueo de sesión, no dejar información confidencial a la vista, etc.

Técnicas

- Auditoría de sistemas: se trata de una medida técnica que permitirá identificar cualquier problema ante la evolución de las infraestructuras. Será un proceso que se ejecutará cada cierto tiempo. Sirva como ejemplo, que una auditoría realizada hace un año, poco o nada tendrá que ver con la situación actual de la empresa ya que los sistemas y aplicaciones pueden haber evolucionado.
- Antimalware: política que obliga a disponer de una solución individual o centralizada para combatir este tipo de amenazas.
- Uso de dispositivos móviles y equipos corporativos: medida que a través de diversas directivas técnicas, tiene como propósito la protección del hardware enumerado.
- Control de acceso: en una empresa u organización, todos los empleados no tienen que tener acceso a "todo", de hecho, tal y como vimos en la unidad 1, ahora se apuesta por el paradigma "Zero Trust". En base a esto, la política establecerá los roles y permisos para poder garantizar los dominios de la seguridad de la información.
- Copias de seguridad: se ha repetido un millón de veces que la información es el activo más importante de una empresa. Este activo está sujeto a una serie de amenazas que pueden afectar a su disponibilidad, integridad o confidencialidad. Las políticas de copias de seguridad deben estar diseñadas para hacer frente a dichos problemas y además debe de estar incardinada en la política de continuidad de negocio.
- Gestión de logs: la monitorización de los sistemas es esencial para garantizar que ante un incidente, podemos dar la respuesta más ágil. Esta política está diseñada para conocer las alertas que se pueden dar, llevar a cabo un análisis que permita identificar el problema y detectar cualquier tipo de error.
- Respuesta a incidentes: con independencia de que hayamos diseñado un excelente plan director de seguridad, es un hecho que los incidentes van a poder materializarse. Un política de este tipo permitirá diseñar un plan de acción y un sistema de escalado para mitigar el problema de una manera ágil. Es muy importante que esta política esté muy bien detallada.
- Actualizaciones: puesto que la entrega o el "delivery" de actualizaciones puede ser muy complejo en organizaciones muy grandes, es vital contar con un plan que impida que un atacante pueda aprovecharse de una vulnerabilidad en un sistema operativo o una aplicación. A través de esta política se diseñará como llevar a cabo el despliegue.
- Borrado seguro: en ocasiones por necesidad, otras por cumplimiento legal (eliminación de datos tras retención obligatoria), será necesario diseñar e implementar un control que permita a la organización destruir la información con total garantía de que no es posible recuperarla.
- Teletrabajo: se trata de una política que tras la aparición de la pandemia se ha hecho muy popular. Básicamente contendrá las directrices necesarias para desempeñar esta modalidad de manera segura. Por ejemplo, conectarse siempre a través de una VPN, usar 2FA, etc.

Existen tantas políticas de seguridad como necesidades identifiquemos en nuestro negocio pero en cualquier caso, es importante que se priorice en función de qué es lo que deseamos proteger.

5.- GUÍAS BUENAS PRÁCTICAS

Es importante distinguir entre una buena práctica y una política. En el caso de las guías, ocurre algo similar. Las empresas van a poder contar con documentos elaborados por diversas organizaciones dedicadas a la ciberseguridad, tanto de ámbito nacional como el INCIBE o el CCN-CERT, como internacional con la ENISA o ECSO, que facilitan numerosas guías de buenas prácticas con muy diversos propósitos. Recordamos que estas no son de obligado cumplimiento pero sí muy recomendables para la implementación de controles específicos sobre los sistemas o redes que queramos proteger.
Las temáticas que ofrecen son muy diversas, desde el uso seguro de las redes wifi hasta recomendaciones específicas para sectores concretos como por ejemplo los fabricantes de juguetes conectados.

No es objetivo de este punto enumerar y explicar el propósito de cada una de las guías disponibles, se facilitan las referencias a los listados más interesantes para que el alumno pueda escoger.

- Guías de ciberseguridad del INCIBE
- Guías STIC del CCN
- Guías de la ENISA
- Guías de ECSO

6.- ESTÁNDARES DE SECURIZACIÓN EN SISTEMAS Y REDES

Caso práctico

Las organizaciones que implementen un estándar de seguridad estarán alineadas con las mejores prácticas desarrolladas por conjuntos de expertos, tendrán más garantías de que los procedimientos funcionen adecuadamente. Además, podrán certificarse en alguno de estos estándares (ej.: ISO27000).

En el punto anterior, hablábamos de medidas que no son obligatorias pero es recomendable implementar, cuando nos referimos a un estándar o un marco específico de securización para las redes y los sistemas, nos encontramos ante un modelo de obligado cumplimiento siempre y cuando, la empresa que lo implemente, quiera certificarse en ese estándar. Como ejemplo sirva una empresa que toma el cuadro de controles de la ISO 27001, para implementar alguno de ellos pero sin certificarse, obviamente lo podrá hacer sin ningún problema, pero en el momento en que quiera certificar su SGSI (Sistema de gestión de la seguridad de la información), deberá cumplir todos aquellos controles que le apliquen.

Partamos mencionando la definición de estándar: ”La legislación (Artículo 8 de la Ley 21/1992 de Industria) define norma como “la especificación técnica de aplicación repetitiva o continuada cuya observancia no es obligatoria, establecida con participación de todas las partes interesadas, que aprueba un Organismo reconocido, a nivel nacional o internacional, por su actividad normativa”. Este concepto cuyo origen parte del ámbito industrial, se ha llevado también a otros contextos, como es el caso de la ciberseguridad y ha venido manteniendo el orden de aprobación a través de organismos conocidos como UNE, ISA, NIST, IEC, entre otras.

Mencionar que también es cierto que existen corrientes que no están demasiado a favor de estas cuestiones pues la implementación de una norma, lleva asociados una serie de costes que no todas las organizaciones pueden asumir. De hecho, la certificación de un SGSI cuenta con unos periodos de revisión en los que hay que desembolsar, además de cumplir los requisitos, una suma de dinero para mantener la certificación.

Estándares más relevantes en el mundo de la ciberseguridad que cubren los aspectos más importantes:

ISO

A continuación las más relevantes relativas a la Internation Standards Organization:

- ISO/IEC 27000: Gestión de la seguridad de la información (SGSI).
- ISO/IEC 27032: Directrices para la ciberseguridad.
- ISO/IEC 27033: Seguridad de la redes.
- ISO/IEC 27034: Seguridad de las aplicaciones.
- ISO/IEC 27035: Gestión de incidentes de seguridad de TI.
- ISO/IEC 27036: Gestión de la seguridad de la información en relaciones con terceros.

NIST Cybersecurity Framework

Debes conocer

El ENS, es un marco normativo de aplicación en la Administración Pública de España, cada vez es más común que en las licitaciones públicas se exija a los contratistas estar certificados en el Esquema Nacional de Seguridad.

7.- CARACTERIZACIÓN DE PROCEDIMIENTOS, INSTRUCCIONES Y RECOMENDACIONES

A continuación, y tomando como ejemplo la gestión de incidentes, se va a proponer un modelo de caracterización pero hay decenas de alternativas. En primer lugar hemos de determinar los elementos esenciales:

- Nombre del proceso/procedimiento: gestión de incidentes
- Propietario: jefe de seguridad (CISO). En este caso, será el que tenga la responsabilidad.
- Cliente/destinatario del proceso: usuarios, personal, clientes, etc. El público al que se dirige.
- Objetivo del proceso: gestionar los incidentes que lleguen a través de la cuenta de correo y procesarlos a través de RTIR. Aunque la descripción es sencilla en este caso, se ha de tener en cuenta cuestiones como la idoneidad del mismo, la obtención de indicadores para medir la eficacia y eficiencia y ver cómo satisfacen las necesidades de los destinatarios.
- Elementos de entrada: colas de correo, llamadas telefónicas y formulario web. Se han de indicar desde dónde llegan los input.
- Elementos de salida: elementos resultantes del proceso como informes, estadísticas, etc.
- Recursos humanos: responsable, tres técnicos de nivel 1 y un técnico de nivel 2. Será el “músculo” para que el procedimiento se lleve a cabo.
- Recursos tecnológicos: cola RTIR, máquinas de pruebas, sandboxes y cuadros de mando Kibana.
- Mecanismos de control: informes de seguimiento y tiempo de respuesta.
- Indicadores: número de incidentes resueltos por día, media de resolución de incidentes, etc. Es importante contar con herramientas de medición ya que lo que no se puede medir, no se puede mejorar.

8.- NIVELES, ESCALADO Y PROTOCOLOS DE ATENCIÓN A INCIDENCIAS

Caso práctico

En la gestión de incidentes es necesario llevar a cabo procesos de escalado. Estos se realizan en función de la importancia del incidente o del impacto que este pueda tener. Si se trata de una amenaza que puede provocar grandes daños, se elevará al equipo más preparado para contenerla.

Comenzaremos mencionando que no existe un método específico para esta cuestión. Puesto que la tipología de incidentes varía a medida que las tecnologías evolucionan, los procedimientos avanzan en pro de estas.
En primer lugar es preciso distinguir entre:

- Evento: cambio de estado de “algo” dentro de la infraestructura TIC, que es significativo. También se puede denominar notificación o alerta.
- Evento de seguridad: se trata de un evento que genera una notificación a raíz de la violación de una política o directiva de seguridad implementada.
- Incidente de seguridad: es un evento o una serie de eventos de seguridad no deseados o no previstos que pueden poner en riesgo a los sistemas de la organización y a la información que almacenan o contienen.

Por lo tanto, identificamos tres tipos de eventos que presumiblemente derivarán en tres tipos de gestión o de escalado. No obstante, antes de proceder a dicha cuestión, será necesario categorizar el tipo de incidente que variará en función de los sistemas que afecte, la criticidad de los mismos, la información que puede comprometer, etc. De hecho, para la clasificación de incidentes, existe una taxonomía común muy interesante que se puede consultar en la página del CERT de INCIBE.

1- Una vez clasificado el incidente y su nivel de criticidad
2- Se procederá a escalar el incidente dónde el procedimiento indique. Por ejemplo, considerando la información y el equipo del punto anterior, los incidentes de tipo bajo, medio y alto, serán resueltos por el nivel 1, mientras que los incidentes de tipo muy alto y crítico, serán resueltos por nivel 2.
3- Tras esta acción, comenzará la fase de procesado del incidente que podría incluir las fases de seguimiento y cierre. Hay que mencionar que el cierre de un incidente, no significa que este se haya resuelto favorablemente. Pongamos como ejemplo un ataque de ransomware para el que no hay herramienta de descifrado y donde la empresa afectada no dispone de copia de seguridad. En ese supuesto se cerraría el incidente sin haberse solucionado el problema y el acceder al pago del atacante, no sería parte de la solución.
4- Para finalizar, en el proceso de gestión de incidentes, es necesario obtener indicadores acerca del servicio para redimensionarlo, para reducir su tiempo de respuesta o para mejorar el servicio.

Respuestas:
Autoevaluación I: b)
Autoevaluación II: b)
Autoevaluación III: a)
TEST I: 1 a), 2 b), 3 d), 4 a), 5 c), 6 b), 7 b), 8 a), 9 x), 10 d)
TEST II: 1 b), 2 b), 3 b), 4 b), 5 a), 6 a), 7 a), 8 a), 9 b), 10 b)

Autoevaluación I

La fase inicial de un análisis de riesgos es:

a) Implementación de medidas
b) Reconocimiento inicial
c) Reconocer el riesgo residual

Autoevaluación II

Las políticas son de obligado cumplimiento mientras que las buenas prácticas:

a) Verdadero
b) Falso

Autoevaluación III

Los indicadores son un elemento fundamental en la caracterización:

a) Verdadero
b) Falso

TEST I

1- Un EDR es una medida técnica de carácter:

a) Preventiva y reactiva.
b) Exclusivamente preventiva
c) Preventiva y de ejecución.
d) Exclusivamente reactiva

2- Existen tres grupos esenciales de medidas técnicas de seguridad ¿Verdadero o falso?

a) Verdadero
b) Falso

3- ¿Qué elemento forma parte de la caracterización de un procedimiento?

a) Climatología
b) Sociedad
c) Propietario
d) Capacidad

4- Un DLP es una medida:

a) Medida técnica
b) Medida global
c) Medida humana
d) Ninguna es correcta.

5- Las herramientas que en caso de que se materialice un incidente, puedan llevar a cabo alguna acción que permita contenerlo, eliminarlo o corregir la situación se denominan:

a) Preventivas y reactivas.
b) Preventivas.
c) Reactivas.
d) Sinérgicas.

6- La respuesta a incidentes y las actualizaciones son políticas de tipo:

a) Organizativa
b) Organizativa y técnica.
c) Técnico.
d) Ninguna respuesta es correcta.

7- En la economía circular, las materia multimaterial son más fáciles de reciclar ¿Verdadero o falso?

a) Verdadero
b) Falso

8- La verificación de que los controles son efectivos pasa por el establecimiento de un cuadro de mando. ¿Verdadero o falso?

a) Verdadero
b) Falso

9- x

10- Dentro de los modelos de madurez CMM ¿Cuál no estaría incluido?:

a) Administrado.
b) Inexistente.
c) Definido.
d) En ejecución

TEST II

1- Un IDS es una herramienta que actualmente tiene muy poca utilidad ¿Verdadero o falso?

a) Verdadero
b) Falso

2- Una copia de seguridad por sí sola, sin verificación, ya es una medida de protección con la que una organización puede considerarse medianamente protegida. ¿Verdadero o falso?

a) Verdadero
b) Falso

3- El propietario no es un elemento de una caracterización de un procedimiento. ¿Verdadero o falso?

a) Verdadero
b) Falso

4- Un IDS es una herramienta de tipo reactivo. ¿Verdadero o falso?

a) Verdadero
b) Falso

5- Para establecer un plan de securización, es necesario conocer la situación actual de la empresa:

a) Sí. Eso permitirá adecuar el plan a la organización
b) Solamente si el sistema informático forma parte del sistema de información seguro.
c) Solamente si el sistema de información forma parte del sistema informático.
d) Nunca.

6- ¿El NIST Framework se puede considerar como un marco de buenas prácticas en ciberseguridad?

a) Verdadero
b) Falso

7- Las medidas preventivas de seguridad se incardinan en:

a) Medidas técnicas.
b) Ninguna es correcta.
c) Medidas legislativas.
d) Medidas incondicionales.

8- "El residuo se convierte en recurso. Todo el material biodegradable vuelve a la naturaleza y el no biodegradable se reutiliza" es un principio fundamental de la economía circular. ¿Verdadero o falso?

a) Verdadero
b) Falso

9- La limitación de alcance, nunca se debe considerar en un análisis de riesgos. ¿Verdadero o falso?

a) Verdadero
b) Falso

10- Las buenas prácticas son de obligado cumplimiento. ¿Verdadero o falso?

a) Verdadero
b) Falso

PRÁCTICA

El alumno debe identificar qué elementos/decisiones/acciones no cuadran con unas prácticas correctas de los planes de securización que pueden provocar problemas.

Escenario:

La empresa "Venus SA", dedicada a la cirugía estética y con sede en Ibiza. El grado de dependencia tecnológica es bajo ya que la mayor parte de la información que gestionan como los historiales de los pacientes se encuentran en formato físico. La empresa cuenta con 10 empleados distribuidos de la siguiente manera:

- Un CEO.
- Un empleado del departamento de RR.HH.
- 5 doctores en cirugía estética.
- 2 empleados encargados de la limpieza y saneamiento de la clínica.
- Un recepcionista.

El CEO de la empresa ha decidido modernizar la clínica para ello se han marcado los siguientes hitos:

- Desarrollar una herramienta informática que gestione:
  - Historiales de los pacientes.
  - Nóminas.
  - Relaciones con proveedores.
- Informatizar todos los historiales.
- Adquirir nuevos equipos con los que poder utilizar la herramienta.
- Crear una página web corporativa de carácter informativo.
- Adquirir un nuevo servidor para alojar la herramienta.
- Reducir al máximo posible los costes y plazos de entrega.

Debido a que el presupuesto es reducido varias empresas con las que se han puesto en contacto se han negado a realizar el desarrollo pero finalmente una empresa local acepta los términos además garantizar costes y plazos.

Transcurrido no más de un mes la empresa desarrolladora ha terminado y deciden presentar al CEO de Venus SA. los resultados de su trabajo. Para ello pactan una reunión en la que los principales puntos tratados fueron:

- Con el fin de reducir costes tanto el programa gestor como la página web corporativa se ubican en el mismo servidor.
- La herramienta que gestiona informes, nóminas y proveedores ha sido desarrollada ex profeso para Venus SA.
- Para la página web corporativa se ha utilizado un gestor de contenidos o CMS de código abierto.
- El servidor se alojará en el cuarto destinado a guardar los productos y herramientas de limpieza.
- Como personal de mantenimiento de la herramienta y la página web se dará una formación al recepcionista de clínica.
- Todos los equipos serán configurados para que los usuarios puedan ser administrados por los propios usuarios.
- Le recomiendan que la informatización de los historiales antiguos la haga el personal interno, como el recepcionista, ya que el proceso es bastante sencillo y principalmente lo que hay que hacer es escanear documentos.

El CEO decide dar luz verde, para que la actualización sea lo menos traumática posible. Esta se realizará durante el fin de semana así como la formación de los empleados. Llegado el lunes, el recepcionista comienza a digitalizar todos los informes, el personal de recursos humanos hace lo propio con las nóminas y el CEO con los proveedores.

Después de una semana de arduo trabajo, sobre todo del recepcionista, el sistema está listo para ser utilizado por los doctores. A los pocos días de uso de la herramienta esta deja de funcionar correctamente y constantemente se producen caídas del servicio pese a los intentos del recepcionista-técnico de sistemas por solucionarlo. Tanto los doctores, como el personal de RR.HH. y el CEO deben volver a hacer su trabajo como lo habían estado haciendo hasta antes de la informatización de la clínica.

Apartado 1: Tarea de investigación

Una vez que conoces los diferentes modelos para aplicar ciberseguridad en una organización, en base al supuesto planteado deberás:

- **Identificar qué elementos/decisiones/acciones no cuadran con unas prácticas correctas de los planes de securización.**
- **Ofrecer las mejores soluciones a los problemas previos.**

Identificar qué elementos/decisiones/acciones no cuadran con unas prácticas correctas de los planes de securización.

La modernización de la clínica Venus SA presenta una serie de errores en su proceso de implementación de tecnología, que afectan tanto a la infraestructura como a la seguridad, la formación del personal y la elección de proveedores. Los errores identificados no solo han expuesto a la empresa a vulnerabilidades tecnológicas, sino que también han impactado directamente en el funcionamiento diario, con constantes caídas del sistema y la incapacidad de resolver los problemas de manera eficiente. Los elementos que no cumplen con una buena práctica son los siguientes:

- Análisis y planificación previos

La modernización de la clínica se inició sin un análisis de riesgos ni un plan estratégico que evaluará las necesidades y los recursos. No se llegaron a identificar los requerimientos técnicos, las normativas de protección de datos, ni se definieron los roles para el personal encargado. Esto derivó en decisiones erróneas y apresuradas que pudieron convertirse en vulnerabilidades para la infraestructura.

- Un único servidor

Al tener bajo presupuesto se comprometió la calidad de la infraestructura. Alojar la herramienta de gestión, que maneja historiales clínicos y nóminas, junto con la página web en el mismo servidor puede suponer un riesgo de seguridad y de rendimiento. Además el servidor se alojó en el cuarto junto con los productos de limpieza, lo que puede suponer un daño físico por la posible suciedad, humedad, accidentes…

- Personal no cualificado

El recepcionista fue elegido como técnico de sistemas y encargado de la digitalización, una tarea que requiere cualificación técnica y comprensión de la sensibilidad de los datos manipulados. Esta decisión infravaloró la complejidad de las funciones y sobre cargó al empleado en el desempeño de sus funciones y el correcto manejo de la informatización.

- Medidas de seguridad

La configuración de los equipos permitió que los usuarios tuvieran privilegios de administrador, lo cual es una mala práctica que facilita errores humanos y posibles ataques. Además, no se implementaron controles de acceso ni cifrado para proteger los datos sensibles. Esto pudo suponer una vulnerabilización de la confidencialidad de los datos, exponiéndolos a accesos no autorizados y pérdida de información.

- Proveedor no especializado

La empresa contratada cumplió plazos irreales, priorizando la rapidez a la calidad. Esto resultó en un software mal diseñado y con fallos, que después ocasionaron caídas del servicio.

- Soporte técnico

No se planificó un servicio de mantenimiento técnico, auditorías, ni la contratación de personal especializado para gestionar el sistema. Se hizo un intento de formar al recepcionista como técnico, lo que demuestra una falta de previsión a largo plazo. Adicionalmente el resto de personal tampoco recibió formación para garantizar el uso eficiente y seguro de las herramientas.

En resumen, los problemas principales surgen de una combinación de decisiones apresuradas, falta de preparación y la subestimación de la complejidad que implica digitalizar datos sensibles. Sin un enfoque adecuado en seguridad, formación y mantenimiento, los esfuerzos de informatización no solo han fallado en alcanzar los objetivos planteados, sino que han dejado a la empresa vulnerable a fallos tecnológicos y riesgos de seguridad.

Ofrecer las mejores soluciones a los problemas previos.

Las soluciones planteadas abordan los problemas identificados, con el objetivo de garantizar una transición tecnológica exitosa y segura para Venus SA. La clave para corregir los errores radica en una planificación sólida, una mejora en la infraestructura tecnológica y la adopción de medidas de seguridad adecuadas. Además, es esencial contar con personal cualificado y proveedores de confianza que garanticen la calidad y estabilidad del sistema en un largo plazo. Las propuestas también incluyen un soporte técnico adecuado y una formación continua para el personal.

1. Planificación y análisis inicial

Realizar un análisis de riesgos y necesidades antes de la implementación del proyecto, que incluya: la identificación de los recursos tecnológicos necesarios (servidores, equipos…), la evaluación de la formación requerida de los empleados, definiendo los roles y el análisis del cumplimiento de normativas de protección de datos.

2. Servidores

Utilizar servidores dedicados y separados para las diferentes funciones, uno para la herramienta de gestión y otro para la página web corporativa. Debemos asegurar que ambos estén ubicados en un espacio adecuado con condiciones controladas como temperatura, humedad…

3. Proveedor cualificado

Elegir una empresa de desarrollo con experiencia que ofrezca un diseño seguro y fiable, respetando plazos y presupuestos realistas que implante estándares de calidad y la seguridad adecuada. Asegurar que la empresa proporcione soporte técnico continuo y actualizaciones periódicas del sistema.

4. Personal especializado

Contratar un técnico de TI especializado para la instalación, configuración y mantenimiento de los sistemas. Además se debe proveer formación especifica al personal que usará las nuevas tecnologías, garantizando que el personal esté cualificado para realizar su trabajo sin comprometer la seguridad.

5. Seguridad de los sistemas

Se debe implementar controles de acceso, asegurando que cada usuario tenga privilegios mínimos según su rol, también cifrar los datos sensibles tanto en tránsito como el almacenamiento para proteger la información de accesos no autorizados. Además, implementar políticas para realizar copias de seguridad automáticas para garantizar la recuperación si se produce algún fallo.

En conclusión, las soluciones propuestas ofrecen un enfoque estructurado y estratégico para corregir las deficiencias actuales, mejorar la seguridad y garantizar el buen funcionamiento de la clínica en el futuro. Al aplicar estas medidas la empresa podrá resolver los problemas inmediatos de caídas del sistema y establecer una base sólida para el manejo seguro y eficiente de la información crítica, mejorando tanto su operatividad como la confianza de sus pacientes.