UNIDAD 1

DESARROLLO DE PLANES DE PREVENCIÓN Y CONCIENCIACIÓN EN CIBERSEGURIDAD

De acuerdo con la ISACA (Information Systems Audit and Association), se define ciberseguridad como una capa de protección para los archivos de información que almacenamos en nuestros dispositivos. También conocida como seguridad informática, se sirve de estándares, protocolos, métodos y reglas creadas para reducir al mínimo los riesgos que puede recibir nuestra red e información contenida en ella. La seguridad informática, entre otros, también se encarga de proteger los ordenadores, servidores, dispositivos móviles y datos de ataques maliciosos.

Un incidente de Ciberseguridad es un evento o serie de eventos inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio; provocando una pérdida o uso indebido de información, interrupción parcial o total de los sistemas, siendo los más comunes, la infección por malware, phishing, etc.

CONCEPTOS BÁSICOS DE CIBERSEGURIDAD

CIA: Principios CIA Los principios sobre los que se apoya la ciberseguridad son tres y se conocen como CIA, en sus siglas en inglés: Confidentiality, Integrity y Availability (Confidencialidad, Integridad y Disponibilidad).

Confidencialidad

Es fácil entender que la confidencialidad es el parámetro que lleva a que una información determinada solo llegue a las manos y conocimiento de quien está destinado o autorizado a conocerla. Este tipo de filosofía se aplica a todos los ámbitos y es un parámetro que ha acompañado a la seguridad de la información a lo largo de la historia.

Esto debe hacerse independientemente de la seguridad del sistema de comunicación utilizado: de hecho, un asunto de gran interés es el problema de garantizar la confidencialidad de la comunicación utilizado cuando el sistema es inherentemente inseguro (como Internet).

En un sistema que garantice la confidencialidad, un tercero que entra en posesión de la información intercambiada entre el remitente y el destinatario no es capaz de extraer ningún contenido inteligible.

Para garantizarla se utilizan mecanismos de cifrado y de ocultación de la comunicación. Digitalmente se puede mantener la confidencialidad de un documento con el uso de llaves asimétricas. Los mecanismos de cifrado garantizan la confidencialidad durante el tiempo necesario para descifrar el mensaje. Por esta razón, es necesario determinar durante cuánto tiempo el mensaje debe seguir siendo confidencial. No existe ningún mecanismo de seguridad absolutamente seguro.

La confidencialidad se crea por el esfuerzo que realiza al menos una de las dos partes implicadas en un proceso para compartir información. Si en algún momento hay un tercero que consigue acceder a esa información que no esté autorizado para ello, se habría violado la confidencialidad. Esto se aplica en multitud de casos, como cuando un cliente compra un producto en una tienda online haciendo uso de una tarjeta de crédito. Todo el proceso está protegido confidencialmente y nadie debería acceder a esa información, pero en casos concretos puede ocurrir.

A nivel de la comunicación digital se pueden implementar sistemas de pero hay otros casos en los que se pueda romper la confidencialidad de un proceso. Los ejemplos son cuantiosos: Alguien publica una información privada públicamente sin la autorización de la persona afectada; Un individuo mira a otro introduciendo el número de seguridad de su móvil o tarjeta de crédito;El acceso a discos duros de una empresa con información confidencial de la misma o Divulgar información privada aún tras la firma de un acuerdo de confidencialidad.

Integridad

La Integridad es la propiedad de la información por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.

Esta característica indica que la información debe mantenerse fiel a como fue concebida en su momento salvo autorización expresa para su modificación. Si un libro se mantiene íntegro con el paso de los años y con múltiples traducciones a varios idiomas sin que cambie el contenido o la esencia del mismo se puede decir que se ha respetado su integridad. Si un documento se modifica alterando los datos sin autorización o un programa o cualquier otro tipo de soporte, en este caso se habrá violado la integridad del mismo. Fomentando la integridad es posible garantizar el valor de la información que se transmite.

Disponibilidad

Se define como la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.

En el sector informático y digital es muy sencillo comprender el objetivo del parámetro de la disponibilidad. Se refiere a la necesidad de que la información, los archivos o programas se mantengan disponibles en todo momento pase lo que pase. Para ello deben existir medidas de soporte y seguridad, canales bien establecidos que permitan que la información sea procesada en el momento en el cual sea necesaria y que no se produzcan interrupciones en los servicios. Cuando un sistema garantiza a sus responsables y clientes la disponibilidad de un servicio o de una información, lo que también está haciendo es evitar situaciones de riesgo y exponerse a ataques.

NORMATIVA DE PROTECCIÓN DEL PUESTO DEL TRABAJO

La gestión de la información empresarial se realiza fundamentalmente desde el puesto de trabajo, tanto desde dispositivos tecnológicos como de forma más tradicional (papel, teléfono,..). De ahí la importancia de concienciar a los empleados y exigir el cumplimiento de ciertas normas para la seguridad en su puesto de trabajo y desde su puesto.

Por una parte el empleado debe conocer los riesgos no tecnológicos, por ejemplo: información en papel al alcance de personas no autorizadas, la falta de confidencialidad de los medios de comunicación tradicionales, el peligro de robo o extravío de los dispositivos extraíbles (pendrives, discos duros externos, etc.), el acceso físico de terceras personas a las zonas de trabajo (repartidores, personal de limpieza, etc.).

Por otra parte desde en muchos puestos de trabajo se tiene acceso a ordenadores, dispositivos móviles y portátiles con conexión a la red de la empresa y al exterior (internet).

Son pues una «puerta de entrada» a la empresa y a sus recursos de información. Es esencial preparar a los empleados para evitar incidentes que puedan iniciarse en su puesto de trabajo, acentuados por desconocimiento o por falta de preparación: accesos no autorizados a los ordenadores y desde ellos a aplicativos de la empresa; infecciones por malware o robo y fuga de datos en formato digital; ataques de ingeniería social, es decir, engaños para manipular a la víctima para obtener información (credenciales, información confidencial,...) o conseguir que realice alguna acción por él (instalar un programa, enviar algunos correos, hacer algún ingreso, etc.).

Para garantizar un uso adecuado de los dispositivos y medios del entorno de trabajo, y minimizar el impacto que todos estos riesgos pueden tener en la empresa, debe implantarse una política de protección del puesto de trabajo. La organización debe facilitar a los empleados las obligaciones y buenas prácticas en materia de seguridad que apliquen a su puesto de trabajo. Esta normativa debe ser firmada por los empleados en su incorporación a la empresa, así como estar siempre disponible y recordar su aplicación de manera periódica.

El objetivo de la normativa de la empresa en relación al puesto de trabajo es garantizar la seguridad de toda la información y los recursos gestionados desde el puesto de trabajo. A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a protección del puesto de trabajo.

La empresa debe contar con una normativa específica que recoja todas las medidas necesarias para proteger el puesto de trabajo, revisando periódicamente su cumplimiento y modificándola si hubiera cambios que la afecten por ejemplo si se cambian los equipos o los sistemas o se adoptan nuevos servicios. También se dará a conocer a los empleados otras políticas relativas a los equipos o servicios que utilicen en su desempeño: correo electrónico, almacenamiento, etc. A continuación se detallan algunos puntos que se pueden tener en cuenta cuando se defina esta política:

Destrucción avanzada de documentación mediante mecanismos seguros. La información obsoleta se destruirá de forma segura según la Política de borrado seguro y gestión de soportes . En particular: mediante destructoras de papel al servicio de los empleados o contratando un servicio externo de destrucción segura, notificando a los empleados de su existencia y obligación de uso, dando a conocer los riesgos asociados a la utilización de papeleras para documentos sensibles (datos personales, información financiera, etc.).

Bloqueo programado de sesión. El personal informático programará un bloqueo automático de sesión en los equipos al no detectarse actividad del usuario en un corto periodo de

tiempo. Adicionalmente se puede contemplar llevar a cabo la programación del apagado general de equipos una vez terminada la actividad empresarial.

Sistema operativo actualizado. El personal responsable de los sistemas aplicará la Política de actualizaciones de software revisando los equipos periódicamente para garantizar su actualización o activando las actualizaciones automáticas.

Antivirus actualizado y activo. El personal responsable de los sistemas aplicará la Política antimalware que incluya la instalación y actualización de herramientas antimalware en todos los equipos y sistemas, y su revisión periódica de manera que se garantice la protección antimalware.

Deshabilitar por defecto los puertos USB. El personal responsable de los sistemas puede deshabilitar por defecto los puertos USB de todos los equipos y solo estarán habilitados para aquellos usuarios que necesiten, de forma justificada y debidamente autorizada, dicha funcionalidad.

Seguridad de impresoras y equipos auxiliares de oficina. El personal responsable verificará que las impresoras y otros equipos conectados a la red o que puedan contener información de la empresa están incluidos en las Políticas de seguridad estarán dentro del perímetro del cortafuegos, se accederá a su panel de configuración mediante contraseña y por canales cifrados; si tienen wifi se ha de configurar su seguridad; si tienen discos duros se revisarán las Políticas de almacenamiento y si tienen conectores USB se deshabilitarán. También si fuera posible, se dispondrá de mecanismos de impresión segura (con contraseña) en las impresoras.

Uso de los medios de almacenamiento. Para que el empleado haga un uso correcto de los dispositivos de almacenamiento disponibles, debe conocer y aplicar la normativa corporativa relativa al almacenamiento local en el equipo de trabajo, almacenamiento en la red corporativa, en la nube y en los dispositivos extraíbles.

Alteración de la configuración del equipo e instalación de aplicaciones no autorizadas. Es un riesgo que el empleado cambie la configuración del equipo o instale las aplicaciones que considere necesarias. Esta modificación podría tener consecuencias de infección de equipos y por lo tanto de pérdida de información. Si el empleado requiere una configuración o software específico para el desempeño de su trabajo, deberá solicitarlo formalmente al equipo informático.

Política de mesas limpias. Conocemos como política de mesas limpias la obligación de guardar la documentación de trabajo al ausentarse del puesto de trabajo y al terminar la

jornada laboral. No se debe dejar información sensible a la vista de personas que pudieran hacer un uso indebido de la misma. El cumplimiento de esta política conlleva: mantener el puesto de trabajo limpio y ordenado, guardar la documentación y los dispositivos extraíbles que no están siendo usados en ese momento, y especialmente al ausentarnos del puesto o al fin de la jornada laboral; no apuntar usuarios ni contraseñas en post-it o similares.

Destrucción básica de documentación mediante mecanismos seguros. Todo el personal debe utilizar las destructoras de papel para eliminar la información confidencial.

No abandonar documentación sensible en impresoras o escáneres. Para evitar que la información acabe en manos no deseadas el usuario debe: recoger inmediatamente aquellos documentos enviados a imprimir, guardar la documentación una vez escaneada, utilizar los mecanismos de impresión segura si los hubiera.

No revelar información a usuarios no debidamente identificados. La información es uno de los activos empresariales más cotizados. Por este motivo es posible que alguien intente obtener parte de esta información (contraseñas de usuario, información de cuentas bancarias, etc.) engañando a un empleado. Esta práctica se conoce como ingeniería social. Los delincuentes se hacen pasar por algún responsable, persona o empresa conocida para que el empleado se confíe y facilite la información que le solicitan empleando para ello una llamada telefónica, el correo electrónico, las redes sociales o mensajes del tipo SMS o Whatsapp.

Obligación de confidencialidad. El empleado debe aceptar un compromiso de confidencialidad relativo a cualquier información a la que tenga acceso durante su participación laboral en la empresa. La obligación de confidencialidad tendrá validez todo el tiempo que se haya exigido en el contrato laboral. La información debe protegerse aun cuando el empleado ya no forma parte de la empresa.

Uso de las contraseñas. El usuario debe seguir la Política de contraseñas: (usuario y contraseña)son confidenciales y no pueden ser publicadas ni compartidas; no deben anotarse las credenciales en documentos ni en cualquier otro tipo de soporte, las contraseñas deben ser robustas, se deben cambiar periódicamente.

Obligación de bloqueo de sesión y apagado de equipo. Para evitar el acceso indebido o por personal no autorizado al equipo del puesto de trabajo el empleado deberá bloquearlo cada vez que se ausente de su puesto y el empleado apagará su equipo al finalizar la jornada laboral.

Uso adecuado de Internet . El empleado debe conocer, aceptar y aplicar la normativa que regula el uso de Internet como herramienta de trabajo con los usos permitidos y prohibidos. También seguirá las recomendaciones de seguridad relativas a la navegación por internet como:verificar que las direcciones (URL) de destino son correctas, verificar que el certificado es válido, cuando se trate de conexiones a entornos seguros (webmail, extranet, etc.) o realicemos transacciones, comprobar que se cumple el protocolo https:// en las páginas donde se trabaje con información crítica.

Obligación de notificar incidentes de seguridad. El empleado debe advertir de cualquier incidente relacionado con su puesto de trabajo:alertas de virus/malware generadas por el antivirus; llamadas sospechosas recibidas pidiendo información sensible; correos electrónicos que contengan virus, pérdida de dispositivos móviles (portátiles, smartphones o tabletas) y dispositivos externos de almacenamiento (USB, CD/DVD, etc.), borrado accidental de información o alteración accidental de datos o registros en las aplicaciones con información crítica, comportamientos anómalos de los sistemas de información, hallazgo de información en ubicaciones no designadas para ello, evidencia o sospecha de acceso físico de personal no autorizado, a áreas de acceso restringido (CPD, despachos, almacenes,…), evidencia o sospecha de accesos no autorizados a sistemas informáticos o información confidencial por parte de terceros y cualquier actividad sospechosa que pueda detectar en su puesto de trabajo.

Cualquier otra que se considere adecuada para la situación de la empresa.

Una vez elaboradas las directrices, los controles se clasificarán en dos niveles de complejidad:

Básico (B): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.

Avanzado (A): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance: Procesos (PRO): aplica a la dirección o al personal de gestión. Tecnología (TEC): aplica al personal técnico especializado. Personas (PER): aplica a todo el personal.

PLAN DE FORMACIÓN Y CONCIENCIACIÓN EN MATERIA DE CIBERSEGURIDAD.

Los puntos clave del plan de formación y concienciación deben ser los siguientes:

Difusión de la política de seguridad. Las normas de seguridad de la información de la organización deben estar correctamente documentadas y al alcance de todo el personal en todo momento.

Concretar el plan de formación. Para garantizar el éxito de nuestro programa formativo, debemos seleccionar los aspectos que queremos que sean cubiertos: procedimientos y controles de seguridad básicos; ·necesidad de conocer y cumplir normas, leyes, contratos y acuerdos; ·seguridad en el puesto de trabajo, aplicaciones permitidas, uso correcto de los recursos, propiedad intelectual, protección datos personales, etc.; ·conciencias a los empleados sobre la existencia y peligros de la ingeniería social; ·responsabilidad personal por acción u omisión y posibles sanciones.

Programas de formación específicos. Es conveniente analizar si se deben desarrollar programas de formación y concienciación especializados para ciertos perfiles de empleados, tales como técnicos de soporte, administradores de sistemas, etc. Además, sería de gran utilidad elaborar una actividad formativa introductoria para los nuevos empleados.

Periodicidad de la formación. Se debe establecer una periodicidad en las actividades formativas y de concienciación. De esta manera conseguiremos tener unos contenidos actualizados en materia de ciberseguridad y reforzaremos las debilidades detectadas o los mensajes de mayor importancia.

Promover una cultura de seguridad de la información. Además de concienciar y formar a nuestros empleados en ciberseguridad, es conveniente exigir a las entidades externas que interactúan con nuestros sistemas de información que sus políticas de ciberseguridad estén alineadas con la nuestra. Intentaremos extender el plan de concienciación a la mayoría de nuestros proveedores y clientes.

Evaluar el aprendizaje obtenido. Consideraremos la necesidad de realizar evaluaciones entre los empleados para determinar el grado de concienciación y formación que han alcanzado.

MATERIALES DE FORMACIÓN Y CONCIENCIACIÓN.

Los empleados son el motor de la empresa, los que hacen posible su funcionamiento. A diario se enfrentan a un entorno de trabajo cada vez más digitalizado, revisando y respondiendo al correo electrónico, procesando facturas y tramitando pedidos online, gestionando procesos a través de aplicaciones en la nube o en dispositivos móviles o realizando tareas de marketing y difusión en redes sociales o a través de la página web. Utilizan la tecnología en el día a día, pero, ¿son conscientes de los riesgos a los que están expuestos y en qué medida estos pueden poner en jaque a la organización?

La mayoría de situaciones que afectan a la continuidad del negocio se deben de alguna forma u otra a la falta de preparación en ciberseguridad de aquellos que tienen que manejar la tecnología. Para suplir esa debilidad las pymes y microempresas pueden utilizar este **kit de concienciación, una herramienta didáctica para concienciar y entrenar a los empleados en el uso seguro de la tecnología**.

El kit de concienciación de INCIBE permite a los empleados podrán acceder a recursos didácticos y herramientas de entrenamiento para evitar los incidentes de ciberseguridad que afectan a las empresas. Este kit ha sido diseñado para que su implantación puedan llevarla a cabo organizaciones de todos los sectores, sin necesidad de tener conocimientos técnicos previos.

El primer paso que llevaremos a cabo, será desplegar uno o los dos «ataques dirigidos» incluidos en el «kit de concienciación». El objetivo de estos «ataques dirigidos» es concienciar a nuestros empleados de los vulnerables que son y que deben ser precavidos a la hora de confiar en los archivos que ejecutan y los correos que reciben.

Se plantean dos ataques dirigidos con vías de ataque diferentes: por correo electrónico o a través de una memoria USB. En ambos casos el archivo a utilizar será el mismo, pero no el medio.

Es importante intentar que la preparación del «ataque dirigido» pase desapercibida para el mayor número de empleados posible y que solo unos pocos (los necesarios) sepan de su existencia.

Una vez terminada la primera fase de ataques dirigidos, se debierá enviar un mensaje a los empleados informándoles del comienzo del programa de concienciación.

Después de distribuir el/los ataques dirigidos incluidos en el «kit de concienciación» y de dejar un tiempo prudencial para que los usuarios hayan tenido la oportunidad de «enfrentarse» a dichas pruebas, se recomienda distribuir en diversas ubicaciones de nuestras oficinas los posters incluidos en el «kit de concienciación».

Para deberán ser imprimidos y colocados en lugares visibles donde el empleado los pueda leer tranquilamente (el ascensor, la sala de café, salas de reuniones, etc.)

Este será también el momento de imprimir y preparar los trípticos que se incluyen en el kit. Se imprimirá un buen número de copias de los trípticos para que el empleado los pueda coger y leer de forma tranquila durante la pausa del café, en su casa, etc.

También puede ser interesante publicar las imágenes en la intranet o enviarlos por correo electrónico de manera escalonada.

Como parte del «kit de concienciación», se incluyen 12 consejos de seguridad. Éstos pueden utilizarse a modo de recordatorio de los materiales y contenidos ya distribuidos.

Los consejos son imágenes que se pueden publicar en el blog interno, en la intranet, pueden ser enviadas por correo electrónico dentro de un marco de formación continua. Puede ser impresas y utilizadas como posters. También pueden ser utilizadas como nuevos fondos de escritorio y/o salvapantallas. Se deja a la empresa la toma de decisión de cómo utilizar estos consejos de seguridad.

Se pueden «publicar» uno dos consejos de seguridad cada mes, pero nunca más porque no se debe saturar a los empleados con excesiva información.

Una idea opcional, es organizar alguna actividad (a criterio de la empresa) que esté relacionada con el consejo que se publica cada mes. De esta manera, conseguimos que nuestros empleados, además de recordar y asimilar estos consejos, se involucren y los apliquen de alguna manera práctica. Algún ejemplo podría ser un premio al mejor puesto de trabajo, al empleado seguro del mes, etc.

Se considera oportuno, una vez pasados unos 6 meses de la puesta en marcha del «kit de concienciación», repetir las pruebas de los ataques dirigidos o realizar una nueva con el fin de que sea algo nuevo para los empleados. Así, si al principio del proceso formativo se realizó el ataque dirigido del correo electrónico, ahora se podría hacer el del pendrive y viceversa. O se podrían lanzar de nuevo los dos ataques.

Con esto conseguimos dos objetivos. El primero, que nuestros empleados recuerden los consejos de seguridad explicados mediante el material del «kit de concienciación», y a nivel corporativo, nos permite evaluar el impacto de dicho Kit en cuanto a la concienciación en Seguridad de nuestra empresa y empleados. Esta fase tendrá una duración aproximada de 5 días laborales.

Una vez se haya implantado el «kit de concienciación», la empresa puede hacernos llegar su experiencia y opinión sobre el proceso de implantación y su utilidad en materia de concienciación de la seguridad de la información.

Invirtiendo cinco minutos en cumplimentar dicha encuesta y enviarla a INCIBE, conseguimos una retroalimentación de información continua y una base sobre la que mejorar nuestro Kit.

La encuesta consta de nueve aspectos a evaluar, con un valor del 1 al 5, donde el 5 se corresponde con la mejor valoración.

AUDITORÍAS INTERNAS DE CUMPLIMIENTO EN MATERIA DE PREVENCIÓN.

Cualquier organización debe realizar los procedimientos de control interno y de gestión de riesgos en su actividad diaria y tomar las decisiones en cuanto al riesgo con base a su cuantificación cualitativa y cuantitativa, con el objetivo de alcanzar los niveles óptimos en cuanto al cos- te/beneficio de asumir o no un riesgo.

Debe poner en funcionamiento todas las medidas técnicas y organizativas necesarias. Los empleados y usuarios (o los propietarios de las aplicaciones sean o no desarrolladas internamente por la organización) deben ser conscientes de que son parte primordial de esta primera línea de defensa. Son el primer objetivo y la puerta de entrada más débil para los “malos”.

Hay tener mucho cuidado con correos electrónicos sospechosos, dispositivos móviles, redes Wifi, redes sociales, etc. Un uso adecuado de los mismos y conforme a las políticas de seguridad de la compañía provee una garantía que minimiza el riesgo existente. Pero esto no es suficiente, también se tienen que im- plantar todas las medidas técnicas (firewall, IDS, gestión de accesos, cifrado de la información, etc.) al alcance de la organización y en consonancia con la información que se maneja.

Debe existir una política del uso seguro y de configuraciones autorizadas, y tareas de revisión automatizada de los equipos y servidores.

Otra posible verificación pasa por enviar un correo con contenido no autorizado a una control 8 también recomienda agregar otras medidas contra el malware que deben estar recogidas en la política, como el bloqueo de USB y la monitorización continúa de los equipos.

Debe existir una política del uso seguro y de configuraciones autorizadas, y tareas de revisión automatizada de los equipos y servidores.

Otra posible verificación pasa por enviar un correo con contenido no autorizado a una cuenta interna, o navegar por una página dentro de una lista negra.

El acceso a la información debe seguir el principio de “necesidad de conocer”. Un perfilado adecuado mitiga el riesgo, pero aun así debemos implantar otros controles, ya que un ataque puede obtener credenciales que tienen acceso a la información. Debemos emprender acciones complementarias, y algunos de los controles que hemos visto nos ayudan: limitar el uso de USB, monitorizar las conexiones o la separación entre redes.

La prueba del control tiene que ser empírica, intentar acceder a información a la que no tenemos acceso por perfil

Se basa en que cada puesto funcional tiene que tener una formación específica en seguridad. Deben identificarse posibles carencias y formar a los empleados. Igualmente, la organización debería tener un programa de concienciación dirigido a todos los empleados, adecuado a las funciones que realizan.

Solicitar la formación recibida del personal de seguridad nos permite identificar las carencias.

Una forma de probar la efectividad es, una vez realizada la acción formativa/concienciadora, enviar un correo tipo phishing para ver la reacción del empleado y los pasos que realiza para denunciar el evento.