LA SEGURIDAD FÍSICA Y SU IMPORTANCIA EN UNA COMPAÑÍA PARA UNA ADECUADA GESTIÓN DE RIESGOS

Vera Salgado Manuel Antonio
vera.manuel@outlook.com
Universidad Piloto de Colombia

Resumen **-** La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático, este suele pasar a un segundo plano cuando se trata de seguridad de la información. La mayoría de las organizaciones se centran en contramedidas de seguridad orientadas a la tecnología, pero no tienen en cuenta un tema muy importante, como lo es la seguridad física la cual debe implementarse correctamente para evitar que los atacantes obtengan acceso físico y puedan robar, eliminar o modificar información de la compañía. Tener firewalls, IPS, IDS, segmentación de red, métodos de cifrado, VPN's, entre otros controles a nivel de software, serían inútiles sin una adecuada seguridad física. La información de este articulo abarca la importancia de la seguridad física junto con las estrategias que deberían tenerse en cuenta para implementar la seguridad física en las instalaciones de una compañía utilizando controles administrativos, técnicos y físicos.

Abstract **-** Physical security is one of the most forgotten aspects when it comes to designing a computer system, this is to take a back seat when it comes to information security. Most organizations focus on technology-oriented security countermeasures, but do not take into account a very important issue, such as physical security, which must be implemented correctly to prevent attackers from gaining physical access and stealing, Remove or modify company information. Have firewalls, IPS, IDS, network segmentation, encryption methods, VPN's, among others, control the level of software, have useless without physical security. The information in this article covers the importance of physical security along with the strategies that can be taken into account to implement physical security in a company's facilities.

Índice de términos **-** activo, amenaza, ataque, consecuencias, controles, información, impacto, políticas, probabilidad, riesgo, vulnerabilidad.

I. INTRODUCCIÓN

La seguridad física en el tiempo se vuelve cada vez más compleja y suele dejarse en un segundo plano para las organizaciones al momento de una adecuada gestión de riesgos. Las nuevas tecnologías y los entornos informáticos cada vez más complejos permiten que se incrementes las probabilidades y brechas de seguridad debido al aumento de las vulnerabilidades. Los discos duros extraíbles USB, memorias USB, computadoras portátiles, tabletas y teléfonos inteligentes permiten la pérdida o el robo de información debido a la portabilidad y el acceso móvil.

En la actualidad, muchas empresas están adaptando en sus oficinas el Coworking, el cual corresponde a grandes espacios compartidos, donde no existe división entre puestos de trabajo, donde los espacios son abiertos con la finalidad de trabajar en colaboración para apoyar el trabajo en equipo, esto implica que se encuentren espacios llenos de computadoras de escritorio y computadoras portátiles que tienen acceso a los datos de toda la empresa. La protección de datos, redes y sistemas se ha vuelto difícil de implementar con los usuarios de dispositivos móviles. Por lo general los comerciales, gerentes y directivos entre otros perfiles, por las funciones correspondientes a su cargo, deben estar en constante movimiento fuera de la oficina, muchos de ellos suelen tener información con datos personales no cifrados de clientes, empleados, proveedores y contratistas, como a su vez información crítica de la organización, toda alojada en sus equipos móviles ya que son fáciles de transportar, lo que los hace más susceptibles al robo o pérdida.

El robo de dispositivos móviles no es la única forma en que los atacantes pueden obtener los datos que desean. Un atacante podría descargar datos confidenciales si conectara un disco duro externo o una memoria USB a una computadora no segura.

Un centro de datos puede estar protegido solo con una guarda de seguridad pero puede pasar que los encargados del cuarto lo dejen por accidente abierto y un atacante acceda al centro de datos. Dejar una memoria USB infectada en el suelo fuera de una oficina de una compañía es otra manera en que un atacante podría robar datos sin tener acceso físico. Existen malware que se pueden propagar en toda la red con solo tener un equipo infectado y puede extraer información a equipos fuera de la red interna o en el peor de los casos, encriptarla y solicitar un pago para su rescate.

El elemento físico de la seguridad a menudo se pasa por alto. Las organizaciones comúnmente se centran en los controles técnicos y administrativos y, como resultado, es posible que los incidentes no se descubran de inmediato. La información tiene diferentes debilidades, riesgos y contramedidas que la seguridad física puede controlar y abarcar. Cuando los encargados de la seguridad de la información tratan de prevenir sobre cómo una persona puede penetrar en la red utilizando medios no autorizados a través de vulnerabilidades inalámbricas, exploits de software o puertos abiertos. Los oficiales de seguridad deben siempre contemplar la seguridad física, les debe generar preocupación cómo controlar o monitorear la forma en que se realiza la entrada física a un edificio o entorno y los daños que un atacante puede causar por no tener o aplicar adecuadamente los controles implementados en la compañía.

La seguridad física pretende proteger personas, datos, equipos, sistemas, instalaciones y activos de la Compañía, Los métodos que protegen la seguridad física de estos activos son a través del diseño del sitio, componentes ambientales, preparación para responder a emergencias, capacitación, control de acceso, detección de intrusos, protección contra incendios y ausencia del fluido eléctrico.

La seguridad física debe planificar y establecer cómo proteger las vidas y las instalaciones de los empleados. La primera prioridad de la seguridad física es garantizar que todo el personal esté a salvo. El segundo es asegurar los activos de la compañía y para finalizar el cómo restaurar las operaciones de TI si ocurre un desastre natural en el menor tiempo posible.

II. PLANIFICACIÓN PLAN DE SEGURIDAD FÍSICA

Para iniciar, la compañía debe identificar al responsable o responsables de crear o mejorar el programa de seguridad física actual de la organización. Esta persona o grupo de personas debe trabajar con la gerencia para definir los objetivos del programa, diseñar el programa y desarrollar métricas basadas en el desempeño y procesos de evaluación para garantizar que los objetivos se cumplan continuamente.

Los objetivos del programa de seguridad física dependen del nivel de protección requerido para los diversos activos y la empresa en su conjunto. Este nivel de protección requerido, a su vez, depende del nivel de riesgo aceptable de la organización. Por lo anterior antes de que se pueda implementar un programa de seguridad física, se debe considerar haber realizado con anterioridad lo siguiente:

- ✓ Haber realizado un análisis de riesgos para identificar las vulnerabilidades y amenazas y calcular el impacto por cada una de ella.
- ✓ Haber trabajado con la administración para definir un nivel de riesgo aceptable para el programa de seguridad física.

El equipo debe presentar los hallazgos a la gerencia respecto al resultado del análisis de riesgos y trabajar con ellos para definir un nivel de riesgo aceptable para el programa de seguridad física. A partir de ahí, el equipo debe desarrollar líneas de base (niveles mínimos de seguridad) y métricas para evaluar y determinar si las líneas de base implementadas se están cumpliendo. Una vez que el equipo identifica e implementa las contramedidas, el desempeño de estas contramedidas debe evaluarse y expresarse continuamente en las métricas creadas previamente. Estos valores de rendimiento se comparan con las líneas base

establecida. Si las líneas de base se mantienen continuamente, entonces el programa de seguridad es exitoso, porque no se excede el nivel aceptable de riesgo de la compañía.

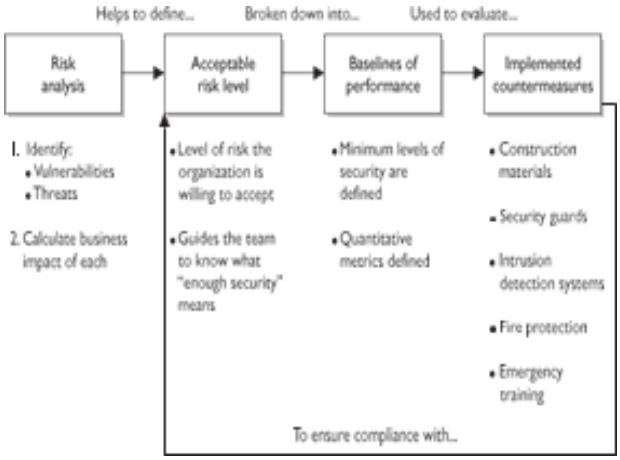

Fig. 1. Relaciones de riesgo, líneas de base y contramedidas
Fuente: CISSP All-in-one Exam Guide

La seguridad física es una combinación de personas, procesos, procedimientos y equipos para proteger los recursos. Aunque cada organización es diferente, el enfoque para construir y mantener un programa de seguridad física es el mismo. La organización antes de iniciar debe identificar sus activos, definir sus vulnerabilidades, amenazas y los agentes de amenaza refiriéndonos a la persona o mecanismo que realmente explota una vulnerabilidad identificada.

Las amenazas se deben dividir en dos categorías, las amenazas internas y externas. Las amenazas internas pueden incluir dispositivos infectados, riesgos de incendio, inundación o empleados internos que pretenden afectar a la empresa de alguna manera. Los empleados internos tienen conocimiento de las instalaciones y los activos de la empresa, que normalmente se requiere para realizar tareas y responsabilidades que con lleva su cargo, esto facilita que el colaborador lleve a cabo actividades dañinas sin que nadie lo note.

Desafortunadamente, una gran amenaza para las empresas puede ser sus propios empleados, que generalmente cuando materializan un evento malicioso, en su mayoría de veces nunca son detectados.

Por otra parte encontramos las amenazas externas, por ejemplo los edificios del gobierno son por lo general los objetivos elegidos para algunos tipos de ataques terroristas. Si una empresa realiza abortos o lleva a cabo experimentos con animales, entonces los activistas suelen ser una amenaza constante. Y, por supuesto, los bancos que son blancos tentadores para los miembros del crimen organizado.

Las organizaciones deben minimizar los riesgos asociados a las vulnerabilidades encontradas en los activos de la compañía y también deben planear como tratar con un riesgo cuando se materialice, en otras palabras, diseñar un adecuado sistema de gestión a incidentes.

Una vez que estos pasos han tenido lugar el equipo está listo para avanzar en su fase de diseño real. El diseño incorporará los controles requeridos para cada categoría del programa; disuasión, retraso, detección, evaluación y respuesta.

III. CONTROLES DE SEGURIDAD FÍSICA

La seguridad física administra y protege los recursos y activos en forma de controles administrativos, técnicos y físicos.

IV. CONTROLES ADMINISTRATIVOS

A. Instalaciones

La primera línea de defensa debe ser controles administrativos, técnicos y físicos y la última línea de defensa siempre debe ser empleados. Limitar la interacción humana con los atacantes reduce el riesgo y la criticidad del evento. Estos controles buscan mantener la seguridad física para proteger a las personas, la infraestructura de TI y las operaciones. Los controles deben ser utilizados para que los atacantes tengan una barrera para detenerlos o retrasarlos.

La seguridad física correspondiente a las instalaciones, es allí donde se identifica y establece las relaciones entre procesos, operaciones y aplicaciones. Un ejemplo podría ser un servidor de archivos de la compañía, este necesita acceso a

internet, energía, control de temperatura, hardware del servidor y ubicación de almacenamiento. En este ejemplo, se identifican los recursos que requieren seguridad. Además, las dependencias e interacciones que respaldan la funcionalidad del negocio se reducen a solo las obligatorias porque se identificaron los procesos, las operaciones y las aplicaciones. La infraestructura de TI incluye computadoras, servidores, equipos de red, agua, electricidad, control de temperatura e infraestructura física.

En mi experiencia como administrador de centros de datos y líder de equipos de tecnología, he encontrado en las empresas, que cuentan con sistemas robustos a nivel de hardware y software pero que no están debidamente protegidos físicamente, un ejemplo de ello es que los cuartos de servidores no cuentan con un adecuado sistema de refrigeración, no tienen protección frente a fluido eléctrico, sin seguridad de control de acceso, con filtración de agua sobre el cuarto donde reposan los servidores, cuartos de servidores con ventanas sin vidrios y con vista a la calle, centros de datos adaptados en donde antes funcionaba un baño y hasta el compartir el cuarto de datos con la señora de oficios generales, todo lo anterior es una deficiencia al momento de diseñar la seguridad física.

B. Instalaciones

La ubicación geográfica, el precio y el tamaño son factores de decisión cuando se contempla en mudarse de una oficina a otra o la apertura de una nueva sede. Los requisitos de seguridad siempre deben ser la principal preocupación al determinar una ubicación tanto para la ubicación de los centros de datos o servidores dentro de una oficina, casa o edificio, como la ubicación de los mismos. Es importante tener en cuenta que pueden producirse saqueos, disturbios, vandalismo y robos. También inundaciones por filtraciones de agua en la infraestructura o por el daño de tubería, sí un cuarto de servidores o de comunicaciones está cerca o dentro de cuartos que tengan circuitos de acueducto, corresponde a una mala decisión de ubicación para los equipos de TI. Otras cosas a considerar antes de determinar un sitio son la visibilidad, incluido el terreno alrededor del edificio, los vecinos y la población del área. La accesibilidad al sitio es importante. El acceso por carretera, el tráfico y la distancia, autopistas y aeropuertos son aspectos importantes. Las áreas geográficas prevalentes a los desastres naturales no son ubicaciones de sitios ideales. Estas amenazas no se pueden evitar porque los desastres naturales no son predecibles, sin embargo el personal de TI, el personal de emergencia, el equipo de gestión y recuperación de desastres, deben estar preparados y equipados para manejar desastres naturales. Los planes de recuperación de desastres contenidos en el plan de continuidad del negocio son el plan general que enumera los detalles necesarios para recuperarse de una tragedia.

C. Diseño

Antes de construir un sitio, diseñar la infraestructura de TI, sistema u otros elementos, los requisitos de seguridad deben ser entendidos. Algunos problemas de seguridad requieren planificación, incluyen el control de acceso para entrada no autorizada, evacuación de emergencia, señalización de entrada y salida, usos de alarmas. Los materiales y métodos de construcción utilizados para construir la instalación deben cumplir o superar los códigos de construcción y las medidas de seguridad. El diseño de la pared debe cumplir con las clasificaciones de fuego mínimas requeridas en diferentes áreas sobre todo para los cuartos de centros de datos y comunicaciones. El tipo de material combustible que se usa y el refuerzo para las obligaciones de seguridad, como proteger las salas de servidores o las áreas que tienen equipos de TI críticos, deben cumplir con los estándares del código. Los mismos principios de diseño se aplican a las puertas, además del diseño de la puerta en la ubicación, cómo las puertas soportan la entrada forzada, será monitoreada por el sistema de alarma, la durabilidad de la bisagra, la dirección de apertura de la puerta y los bloqueos necesarios.

El diseño del techo tiene en cuenta el material combustible utilizado, clasificación de incendios y peso. Los límites máximos requieren consideraciones especiales. Por ejemplo, una pared separa a un atacante de su objetivo. El techo en

ambas habitaciones es de tipo techo colgante o techo falso y la pared no se extiende mucho más allá de las baldosas. El atacante solo necesita escalar la pared para lograr su objetivo.

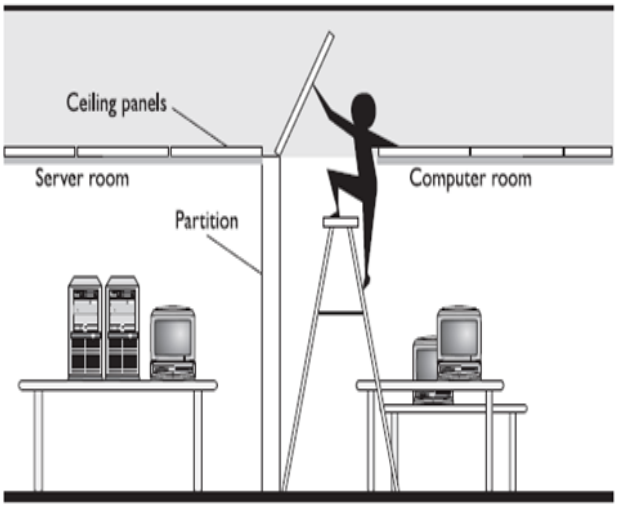

Fig. 2. Un intruso puede levantar los techos falsos e ingresar a un área segura con poco esfuerzo
Fuente: CISSP All-in-one Exam Guide

El diseño de ventana debe contemplar sí las ventanas deben estar protegidas por un sistema de alarma, que sean claras, oscuras, escarchadas o irrompibles. El diseño también debe tener en cuenta si los intrusos pueden obtener acceso a través de ellas. Los planos de diseño de pisos para el tipo de material combustible a usar, peso que el piso puede soportar e indicar sí el piso es estándar o elevado. En un entorno de piso elevado o piso falso, el espacio accesible debajo del piso se usa principalmente para agregar cableado eléctrico o de comunicaciones.

El diseño de calefacción, ventilación y aire acondicionado detalla la ubicación del sistema central y los respiraderos, interruptores y valores que se pueden desconectar en situaciones de emergencia. El diseño de los sistemas eléctricos incluye energía constante regulada, alimentadores dedicados para proporcionar grandes cantidades de electricidad si es necesario, la ubicación de los paneles eléctricos principales y secundarios, y las fuentes de energía alternativas. El diseño del gas y el agua debe determinar la ubicación de las válvulas de cierre, la colocación de tuberías de agua subterráneas y líneas de gas.

D. Prevención del crimen ambiental

La prevención del delito a través del diseño ambiental (Crime prevention through environmental design – CPTED) intenta reducir el delito utilizando la construcción de instalaciones, elementos ambientales y procedimientos para modificar el comportamiento humano. Este modelo de diseño ha mejorado debido a la necesidad debido a que los tipos de delitos y el entorno han evolucionado. Por ejemplo, ahora las personas malintencionadas pueden fingir estar hablando por su teléfono celular mientras realizan un reconocimiento de video. Un ejemplo de CPTED es que los servidores de misión crítica localizados cerca de una pared exterior deben moverse en caso de una fuerza externa hacia el medio del edificio donde hay menos posibilidad de impacto. Por otra parte las cámaras de vigilancia deben colocarse a plena vista, sí los adversarios saben que están siendo monitoreados lo van a pensar antes de ejecutar el plan malicioso y pueden estar cambiando de objetivo. Los empleados se sienten más seguros sabiendo que hay menos posibilidades de un incidente.

El endurecimiento o protección de los activos también se centra en la prevención del delito. Difiere de CPTED en utilizar alarmas, puertas, cerraduras, cercas y conceptos similares para denegar el acceso a través de barreras artificiales y físicas. Cuando se utiliza el endurecimiento de objetivos, la vista del entorno es menos atractiva.

E. Asegurar los centros de datos

Los centros de datos y las salas de servidores que alojan equipos informáticos o de comunicaciones deben estar fuera de los límites de las personas no autorizadas, estos cuartos no deben tener tubería de agua ni en sus paredes laterales, como en el techo, se debe garantizar que en el piso de arriba no existan baños ya que por inundación se pueden ver afectados por filtración de agua. Estas salas deben estar bloqueadas para evitar ataques, solo deben tener acceso el personal autorizados para la ejecución de sus labores para las que fueron contratados. Estas salas de centros de datos almacenan equipos de misión crítica y por lo tanto debe considerarse ser ubicados en el medio de las instalaciones, no en el sótano ni en plantas

superiores. Deben estar protegidas por sistemas de control de acceso biométrico por huella, contraseña o tarjeta, contar con sistemas de detectores de humo, tener extintores adecuados para equipos eléctricos, estar monitoreados por circuitos cerrados de televisión, detectores de movimiento y aires acondicionados para garantizar temperaturas bajas que hacen que los equipos trabajen adecuadamente.

Hay empresas que utilizan iluminación extremadamente tenue, temperaturas frías y espacios reducidos para dificultar la movilidad en esos cuartos, son métodos utilizados para crear un entorno inhóspito humano.

V. CONTROLES FÍSICOS

Las instalaciones necesitan controles de acceso físico que controlen, monitoreen y administren el acceso. La categorización de las secciones del edificio, sede u oficinas debe ser restringida, privada o pública. Se necesitan diferentes niveles de control de acceso para restringir las zonas a las que cada empleado puede ingresar dependiendo de su función. Existen muchos mecanismos que permiten el control y el aislamiento de los privilegios de acceso en las instalaciones. Estos mecanismos están pensados para disuadir y detectar el acceso de personas no autorizadas.

A. Perímetro de seguridad

Rejas, cercas, compuertas y torniquetes se utilizan fuera de las instalaciones para crear una capa adicional de seguridad antes de acceder al edificio. Las cercas y rejas distinguen los límites claros entre las áreas protegidas y las públicas. Los activos protegidos dictan los niveles de seguridad necesarios de las rejas. Los tipos de rejas incluyen alambre eléctrico, alambre de púas, calor, movimiento o detección láser, concreto y rayas pintadas en el suelo.

Las puertas son puntos de entrada y salida a través de una reja. Para ser un elemento de disuasión eficaz, las puertas deben ofrecer un nivel mayor de protección a las rejas; de lo contrario, las personas malintencionadas tienen la oportunidad de eludir la cerca o reja y usar la puerta como punto de intrusión. La construcción de puertas debe consistir en bisagras endurecidas, mecanismos de cierre y dispositivos de cierre. Se puede contemplar guardias de seguridad o perros. Las cámaras deben monitorear las puertas las veinte cuatro horas del día.

Los torniquetes son un tipo de puerta que permite el ingreso de solo una persona. Los torniquetes funcionan girando en una dirección como una puerta giratoria y permiten que una persona salga o ingrese a las instalaciones a la vez.

B. Identificaciones

La prueba de identidad es necesaria para verificar si una persona es un empleado o visitante. Se recomienda utilizar tarjetas de identificación. Las identificaciones también pueden ser tarjetas inteligentes que se integran con los sistemas de control de acceso, este tipo de control determina hasta qué punto puede llegar a acceder un usuario dentro de la compañía.

C. Detectores de movimiento

Los detectores de movimiento ofrecen diferentes opciones de tecnología según la necesidad. Se usan como dispositivos de detección de intrusos y funcionan en combinación con sistemas de alarma.

D. Alarmas de intrusión

Las alarmas monitorean varios sensores y detectores. Estos dispositivos son contactos de puertas y ventanas, detectores de rotura de cristales, detectores de movimiento, sensores de agua, etc. Los cambios de estado en los dispositivos activan la alarma. En sistemas cableados, las alarmas notan los cambios en el estado del dispositivo creando un cortocircuito. Los tipos de alarmas son para disuadir, repeler y notificar. Las alarmas de disuasión intentan dificultar que los atacantes accedan a los recursos principales cerrando las puertas y activando las cerraduras. Las alarmas repelentes utilizan sirenas sonoras y luces brillantes para intentar expulsar a los atacantes del sitio. Las alarmas de notificación envían señales de alarma a través de módems de acceso telefónico, acceso a Internet o medios GSM (celular). La salida de la sirena puede ser silenciada o audible dependiendo de si la organización está tratando de atrapar

delincuentes en el acto.

VI. CONTROLES TÉCNICOS

El foco principal de los controles técnicos es el control de acceso porque es una de las áreas de seguridad más comprometidas. Las tarjetas inteligentes son un control técnico que puede permitir el acceso físico a un edificio o sala segura y conectarse de forma segura a redes y computadoras de la compañía. Se necesitan varias capas de defensa para superponerse para protegerse de los atacantes que obtienen acceso directo a los recursos de la compañía. Los sistemas de detección de intrusos son controles técnicos que son esenciales porque detectan una intrusión. La detección es obligatoria porque notifica los incidentes de seguridad. El conocimiento del evento le permite a la organización responder y contener el incidente. Los registros de acceso deben monitorearse continuamente, permiten a la organización localizar dónde se producen las infracciones y con qué frecuencia. Esta información ayuda al equipo de seguridad a reducir las vulnerabilidades.

A. Tarjetas inteligentes

Las tarjetas inteligentes tienen microchips y circuitos integrados que procesan los datos. Este control de autenticación ayuda a evitar que los atacantes o empleados no autorizados accedan a sitios a los que no se les permite ingresar. La información del empleado se guarda en el chip para ayudar a identificar, autenticar a la persona y validar sí tiene o no el acceso autorizado donde se está autenticando, ya que por este medio se otorgan permisos de acceso a las diferentes instalaciones de la compañía.

Las tarjetas inteligentes de acceso vienen en dos tipos, de contacto y sin contacto. Las tarjetas inteligentes de contacto tienen un punto de contacto en el frente de la tarjeta para la transferencia de datos. Cuando se inserta la tarjeta, los dedos del dispositivo establecen una conexión con los puntos de contacto del chip. La conexión al chip lo alimenta y permite la comunicación con el dispositivo receptor. Las tarjetas inteligentes sin contacto usan una antena que se comunica con ondas electromagnéticas. La señal electromagnética proporciona energía para la tarjeta inteligente y se comunica con los lectores de tarjeta.

Los sistemas de control de acceso usan lectores de proximidad para escanear tarjetas y determina si tiene acceso autorizado para ingresar o salir de una instalación o área. Los sistemas de control de acceso evalúan los permisos almacenados dentro del chip enviado a través de la identificación por radiofrecuencia RFID. Esta tecnología utiliza el uso de transmisores (para enviar) y emisores (para recibir). En el control de acceso físico, se utiliza el uso de lectores de proximidad y tarjetas de control de acceso que contienen etiquetas pasivas. Las etiquetas pasivas se alimentan desde los lectores de proximidad a través de un campo electromagnético generado por el lector de tarjetas. Se envía una señal al lector cuando se pasa una tarjeta. La puerta se desbloquea una vez que se recibe y se verifica la señal. Estos se suelen utilizar para rastrear artículos de gran valor. Los lectores pueden rastrear movimientos y localizar elementos cuando están conectados a la red y sistemas de detección. Si se elimina un activo de ciertas áreas, la organización puede hacer que el sistema de control de acceso active una alarma.

B. Detección de intrusos, guardias y CCTV

Los sistemas de detección de intrusos (IDS) pueden monitorear y notificar las entradas no autorizadas. Los IDS son esenciales para la seguridad porque los sistemas pueden enviar una advertencia si ocurre un evento específico o si se intentó el acceso en un momento inusual.

Los guardias son una parte importante de un sistema de detección de intrusos porque son más adaptables que otros aspectos de seguridad. Los guardias de seguridad pueden ser ubicados en un lugar específico o hacer rondas patrullando ciertas áreas. Al hacer rondas, los guardias pueden verificar que las puertas y ventanas estén cerradas. Los guardias pueden ser responsables de mirar IDS y CCTV, pueden reaccionar ante actividades sospechosas.

Los sistemas de vigilancia o televisión de circuito

cerrado utilizan cámaras y equipos de grabación para brindar protección visual. En áreas que las cámaras monitorean, es esencial tener suficiente luz. Existen cámaras estilo domo que tienen la capacidad de moverse en todas las direcciones, así como acercar la imagen. Las cámaras PTZ son las mejores para rastrear sospechosos porque la cámara detecta y sigue automáticamente a un sospechoso. Las cámaras PTZ pueden rastrear automáticamente objetos en movimiento a través de métodos mecánicos o de aplicación. Las cámaras que usan aplicaciones de software tienen la capacidad de cambiar los objetivos y pueden filtrar las imágenes estacionarias, lo que permite ahorrar ancho de banda y almacenamiento.

Los grabadores de video digital (DVR) son encargados de digitalizar y grabar las imágenes y audios que llegan desde las cámaras de seguridad. Los DVR incluyen un software que permite ver en una pantalla todas las cámaras de seguridad, elegir que o cuales cámaras ver a la vez, agrandar o achicar los tamaños de las imágenes, mover las cámaras, programar horarios de grabación y programar grabación por detección de movimiento.

C. Vida y seguridad ambiental

Para la seguridad física lo más importante es proteger la vida humana, la primera prioridad en un programa de seguridad física debe ser el cómo prevenir que los empleados sufran algún tipo de lesión y como proteger los elementos ambientales básicos de sus instalaciones.

Los elementos esenciales ambientales básicos deben conservarse para mantener la seguridad de los empleados. Las amenazas a la vida humana y la estabilidad del sitio pueden ser el resultado directo de desastres naturales, la liberación de materiales tóxicos, inundaciones o incendios. El equipo de respuesta a incidentes de seguridad física debe contar con procedimientos establecidos para salvaguardar la vida contra este tipo de eventos. La primera acción requerida es enfocarse en la seguridad humana. En segundo lugar, la restauración de los servicios necesarios para las operaciones de TI puede tener lugar después de que se cumplan todas las medidas de seguridad. En casos extremos, como desastres naturales, deben existir pautas y planes para enfrentar adecuadamente la situación.

Los planes de emergencia son guías que ayudan a mantener la seguridad de los empleados después de que ocurre un desastre natural. Describe cómo disminuir las amenazas a la vida humana, evitar lesiones, hacer frente a la coacción y defender la destrucción de la propiedad en caso de que un incidente físico perjudicial afecte el sitio. Los planes de emergencia solo se dirigen al personal y limita el daño a la propiedad. La planificación de la continuidad del negocio (BCP) y la planificación para la recuperación ante un desastre (DRP) abordan el negocio y la funcionalidad de TI.

D. Electricidad

La continuidad del fluido eléctrico y una señal eléctrica limpia es necesaria para que los equipos electrónicos puedan funcionar correctamente. Las organizaciones necesitan soportar su operación con ayuda de equipos especializados para hacer frente a problemas de la ausencia del fluido eléctrico y a la "Potencia sucia". "Potencia sucia" es un término que se refiere a la electricidad que tiene ruido, irregularidades de voltaje y anomalías de frecuencia. Se debe contemplar usar sistemas de fuente de alimentación ininterrumpida (UPS) para gestionar los asuntos correspondientes a las malas señales eléctricas y garantizar el fluido eléctrico cuando estos fallen. Los sistemas UPS toman electricidad y la almacenan usando baterías. Luego, el sistema genera electricidad limpia y regulada que es esencial para los equipos electrónicos. Con la energía almacenada dentro de las baterías, el sistema electrónico puede funcionar en caso de un corte de energía. Los sistemas UPS proporcionan electricidad durante un tiempo limitado, pero pueden permitir el apagado adecuado de los sistemas informáticos si es necesario. El equipo electrónico también se daña debido a irregularidades de voltaje. Los reguladores de voltaje mantienen los voltajes consistentes, y el uso de protectores de sobre voltaje debe ser utilizado para proteger contra incidentes de alto voltaje.

E. Agua

Las inundaciones y las fugas de agua pueden

causar daños sustanciales a los componentes electrónicos y a cualquier dispositivo que utilice electricidad, especialmente si está en uso. Los sótanos o instalaciones cerca de tuberías que transportan agua nunca deben albergar servidores, centros de datos y otros dispositivos electrónicos críticos. El uso de sensores de agua se debe aplicar en ubicaciones importantes del equipo para detectar agua, sobre todo si cerca hay centros de datos o similares. El personal de seguridad, los equipos de emergencia o funcionarios encargados, deben estar al tanto de la ubicación de las válvulas de cierre de agua y las ubicaciones de drenaje para ayudar a disminuir el daño a las instalaciones.

F. Prevención, detección y supresión de incendios

Los sistemas de humo, fuego, calor y detección deben estar en su lugar para proteger a los empleados de lesiones. Mantener a la gente a salvo es el objetivo más importante del plan de seguridad física. Los sistemas de supresión se ponen en marcha para limitar el daño causado por el humo, el fuego y el calor. Si se aplica demasiada supresión, estos sistemas pueden dañar la infraestructura y las instalaciones de TI.

El triángulo del fuego representa los elementos necesarios para que se produzca la combustión, es necesario que se encuentren presentes los tres lados del triángulo para que un combustible comience a arder, calor oxígeno y combustible.

Fig. 3. Triangulo del fuego
Fuente: extintoressecom.mx

La reacción química ubicada en el centro representa el cambio que ocurre durante los incendios. Sí se elimina cualquiera de los cuatro elementos, reacción química, oxígeno, combustible y / o calor, el fuego puede ser eliminado. Se necesitan diferentes métodos para combatir el fuego, la temperatura puede reducirse con el agua y los polvos secos como el ácido de soda. El monóxido de carbono se usa para minimizar el oxígeno y los gases no inflamables, como el halón u otros sustitutos equivalentes, restringe la reacción química y reduce el suministro de oxígeno. Los incendios pueden propagarse rápidamente y cuanto antes se detecte el fuego, más fácil será extinguirlo y reducir el daño causado. El entrenamiento de conciencia sobre el fuego debe ser una parte obligatoria en el plan de seguridad física. Los empleados necesitan conocer las rutas de evacuación para salir de las instalaciones y dónde reunirse (punto de encuentro) para poder tomar asistencia, de modo que los empleados de seguridad sepan si falta personal. El entrenamiento de conciencia de seguridad debe incluir instrucciones sobre el uso apropiado y la ubicación de los extintores de incendios.

G. Extintores

Los incendios pueden venir en diferentes tipos. Identificando el tipo de fuego se debe saber qué tipo de extintor se necesita para suprimirlo. Usar extintores incorrectos puede intensificar el fuego y empeorar la situación. Existen diferentes tipos de extintores que se clasifican de acuerdo al tipo de fuego a extinguir.

Los hay para materiales ordinarios como la madera, papel y basura, y estos reciben la clasificación tipo “A” por lo regular se representa con la imagen de un bote de basura con llamas extendiéndose por la parte superior y un campo de fuego contra un fondo azul.

Los extintores que se utilizan para el fuego ocasionado por aceites o líquidos inflamables se clasifican como tipo “B” y se representan con la imagen de un bote de gasolina frente a llamas contra un fondo azul.

Los extintores que se usan en fuegos ocasionados por corrientes eléctricas reciben la clasificación tipo “C” y pueden estar etiquetados con la imagen de una conexión eléctrica junto a un enchufe con llamas, extendiéndose en la toma de corriente, contra un fondo azul.

Los extintores que se utilizan para metales combustibles se clasifican como tipo “D” y estas unidades llevan una etiqueta con una “D” dentro de una estrella de cinco puntas amarilla.

Los extintores que se utilizan para aceites vegetales o grasas animales. Requieren extintores especiales para fuegos Clase K, que contienen una solución acuosa de acetato de potasio que en contacto con el fuego producen un efecto de saponificación que enfría y aísla el combustible del oxígeno.

Fig. 3. Triangulo del fuego
Fuente: blog.elinsignia.com

VII. SEGURIDAD DEL PUESTO DE TRABAJO

El puesto de trabajo es el espacio definido por la organización para que un funcionario desempeñe sus labores y obligaciones para las que fue contratado, en este espacio dispondrá de herramientas de trabajo para ejecutar actividades.

Una vez fueron definidos que tipos de controles son necesarios de implementar en la compañía en las tres categorías propuestas con el propósito de mitigar los riesgos asociadas a la seguridad física, se debe fortalecer la seguridad a su vez con medidas de seguridad para los puestos de trabajo, pueda que se tengan todos los controles implementados pero se debe tener presente que los incidentes de seguridad en su mayoría de casos se generan dentro de la propia organización, tanto de manera intencionada como accidental.

Un funcionario no necesita realizar complejos ataques para acceder a la información, basta con hacer parte de la compañía. Las empresas confían de la buena fe y profesionalismo para que cada usuario haga uso apropiado de la información. Al hacer parte de la compañía el usuario ya tiene la autorización para acceder a la información y tenerla a su alcance.

El concepto de puesto de trabajo va más allá de la ubicación física donde el usuario desempeña sus funciones diarias. Dentro de este entorno podemos identificar elementos con relación directa a la seguridad de la información: equipos de trabajo, smartphones, tabletas, dispositivos de almacenamiento extraíbles, impresoras, escáneres, documentación, archivadores, etc.

Mitigar los riesgos asociados a los puestos de trabajo enfocados a la seguridad física, no requieren de inversión económica o gran esfuerzo de los funcionarios encargados de dicha responsabilidad, basta con establecer una cultura de la seguridad de la información y poner en marcha medidas técnicas que son en la mayor parte de los casos sencillas.

Los riesgos asociados a los puestos de trabajo que deben tener en cuenta los equipos de TI o los oficiales de seguridad pueden ser la fuga de información, pérdida o robo de información confidencial, infecciones por malware por descuidos o malas prácticas asociadas al uso del correo electrónico.

Las fugas de información que se producen en las empresas tienen como origen los puestos de trabajo de un empleado. Pueden ser fruto tanto de actos mal intencionados por parte de los empleados descontentos, errores al utilizar los sistemas con los que se gestionan información, no bloquear los equipos al ausentarse del puesto, tener escrita la contraseña en papeles sobre el escritorio, no tener control sobre el almacenamiento de medios extraíbles, entre otros.

Un puesto de trabajo sin las correctas medidas de seguridad puede ser la puerta de entrada a la red corporativa para un atacante.

Las medidas de seguridad que propongo a implementar para proteger el puesto de trabajo tienen un costo de implementación y mantenimiento

muy bajo, que aportarán una mejora sustancial al plan de seguridad física y sobre todo brindar tranquilidad.

H. Controles de carácter organizacional

Lo ideal es contar con una política de seguridad de la información, sino existe, se debe crear con el objetivo de transmitir a los empleados las obligaciones y buenas prácticas en relación con la seguridad de la información con énfasis en los puestos de trabajo.

Las medidas planteadas en la política y normativas de seguridad deben comunicarse a los usuarios de la manera adecuada. Esta documentación debe estar disponible para los usuarios, puede ser en la intranet corporativa como en un repositorio de información compartido, debe ser enviada periódicamente mediante comunicaciones por correo electrónico y darlas a conocer al comienzo de la relación laboral con la compañía.

Debe existir un ***acuerdo de confidencialidad*** que notifique la obligación que tiene los empleados en relación con cualquier información con la que pueda llegar a tener acceso para mantener la confidencialidad de la misma.

Los empleados tienen la obligación de notificar los incidentes de seguridad dentro de la empresa como en el exterior. Estas pueden ser:

- ✓ 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.).
- ✓ Cualquier actividad sospechosa que pueda detectar en su puesto de trabajo.
- ✓ Borrado accidental de ficheros.
- ✓ Alteración accidental de datos o registros en las aplicaciones con información crítica.
- ✓ Hallazgo de información en ubicaciones no designadas para ello.
- ✓ Evidencia o sospecha de acceso físico de personal no autorizado, a áreas de acceso restringido.
- ✓ Evidencia o sospecha de accesos no autorizados a sistemas informáticos o información confidencial por parte de terceros.

Una medida muy usada y efectiva es que la política de seguridad es ***prohibir que los empleados publiquen o compartan sus contraseñas***. Las claves son elementos confidenciales y deben permanecer en secreto, ya que sólo así se puede garantizar la confidencialidad y trazabilidad de las acciones. Por tanto, las contraseñas nunca deben compartirse ni apuntarse en documentos, ni en cualquier otro tipo de soporte físico que pueda llegar a ser utilizado por un atacante.

Todos ***los empleados tienen la obligación de bloquear sus equipos al ausentarse de sus puestos de trabajo***, así sea para ir a tomar un café, sin embargo el equipo de TI debe utilizar herramientas que garanticen que con cierto tiempo de inactividad en el computador, el sistema se bloquee automáticamente.

Las organizaciones deben ***limitar el un uso de los medios de almacenamiento extraíble***. La utilización de pendrives y discos duros externos es una práctica habitual que conlleva un alto riesgo de pérdida y robo de información.

Se deben deshabilitar por defecto los puertos USB y habilitarlos en aquel personal que necesite dicha funcionalidad de manera periódica, en su reemplazo se pueden utilizar recursos compartidos para el intercambio de la información.

En los casos de que sea necesario el uso de dispositivos de almacenamiento extraíble, se debe transmitir al empleado la necesidad de aplicar ciertas precauciones, como utilizar mecanismos de cifrado que impidan el acceso a la información en caso de pérdida o proteger los archivos por contraseñas robustas.

Cuando el personal de TI entregue los equipos a un empleado que va a iniciar sus labores en la

compañía, deben garantizar que ***los usuarios no puedan alterar la configuración del equipo*** y la instalación de aplicaciones no autorizadas. El usuario final debe ser disuadido de modificar los dispositivos corporativos para instalar nuevas aplicaciones o modificar la configuración del sistema ya que pueden disuadir controles ya implementados tales como los firewall o proxy's.

Toda la documentación física que se haya gestionado durante el día debe guardarse de manera adecuada durante ausencias prolongadas. Los usuarios tienen la obligación de ***guardar la documentación de trabajo al ausentarse del puesto de trabajo*** y al terminar la jornada laboral, lo anterior se conoce como Política de mesas limpias y es un control que se menciona en el Anexo A de la norma ISO 27001.

Esto es especialmente importante para las compañías que trabajan en entornos compartidos con otras empresas o compañeros de la misma empresa, o incluso públicos tales como oficinas de atención al cliente. De esta manera se puede evitar fuga de información, además del robo de documentos que pueden contener información confidencial.

Una política de mesas limpias requiere que:

- ✓ El puesto de trabajo esté limpio y ordenado.
- ✓ La documentación que no se esté utilizando en un momento determinado debe estar guardada correctamente, especialmente cuando el usuario se aleja del puesto de trabajo y al finalizar la jornada laboral.
- ✓ No haya usuarios ni contraseñas apuntadas en post-it o similares.

Las compañías deben contar con mecanismos seguros que estén a disposición de los funcionarios para una adecuada destrucción de documentación física, tales como destructoras de papel para destruir documentación que pueda contener información sensible, obsoleta o innecesaria.

Por otro lado, los empleados deben conocer los riesgos asociados a la utilización de papeleras comunes para documentos sensibles, como datos personales, información financiera, etc. Los funcionarios deben ser notificados y tienen la obligación de no abandonar documentación sobre las impresoras o escáneres, es muy común que un usuario envíe un documento a la impresora y lo recoja más tarde, o que lo imprima a través de la impresora de otro departamento, por cuestiones técnicas, mayor calidad o funcionalidades especiales. Durante ese tiempo la documentación permanece a disposición de otros usuarios, que pueden recogerla accidental o intencionadamente. Se recomienda utilizar mecanismos en las impresoras para que solo salgan las impresiones cuando el usuario digite una contraseña ligada a su usuario, esto evita que estén a la mano documentos sensibles y se pierda la confidencialidad.

Para tener un poco de control sobre el uso correcto de los canales de internet y el correo electrónico, se debe informar a los usuarios las políticas implementadas en cada compañía, así como las posibles sanciones y acciones a tomar en caso de detectarse un mal uso.

I. Controles de carácter técnico

Implementar políticas de contraseñas robustas para los diferentes sistemas de información, esto evita que los funcionarios no elijan contraseñas fáciles de adivinar tales como las primeras letras del abecedario en conjunto con números consecutivos, por ello se deben contemplar los siguientes criterios para la asignación de una contraseña:

- ✓ Una contraseña debe tener como mínimo 8 caracteres que contenga al menos un número, una mayúscula, una minúscula y un carácter especial
- ✓ No debe tener letras consecutivas del nombre del funcionario
- ✓ Deben tener fecha de caducidad, lo ideal es que cada tres meses los sistemas soliciten el cambiar la contraseña.
- ✓ Los usuarios deben ser bloqueados al registrar 3 intentos fallidos de acceso a los diferentes sistemas o aplicaciones.

Hay una medida de seguridad por encima de todas las descritas anteriormente, que es la de la involucración y concientización de los usuarios que hacen uso de los activos de la empresa.

Deben llevarse a cabo programas periódicos de concientización que insistan sobre la importancia de las medidas incluidas dentro de la política de seguridad interna y seguridad física de la empresa para conseguir que los empleados las interioricen y acepten.

VIII. CONCLUSIONES

Los controles administrativos, técnicos y físicos implementados adecuadamente permiten a una compañía administrar y proteger a sus funcionarios y activos que almacenan y administran información.

Para mitigar los riesgos asociados a la seguridad física es necesario establecer medidas de seguridad adaptadas a las necesidades del negocio.

La implementación de controles, junto a un adecuado plan de formación y concientización de los empleados que gestionan la información, ayudará a proteger de manera adecuada las compañías minimizando los riesgos.

Los empleados son el activo más importante de una empresa y el plan de seguridad física tiene la responsabilidad de salvaguardar su integridad. La seguridad del empleado siempre debe ser la prioridad y luego si se debe asegurar las instalaciones.

La implementación y divulgación de políticas dentro de las compañías son un tipo de control eficaz que no requiere de inversión económica y ayudan a mitigar los riesgos asociados la fuga, pérdida o robo de la información.

REFERENCIAS

[1] Wail gum, T. (2005, February 1). Metrics for Corporate and Physical Security Programs | CSO Online. Sitio web: http://www.csoonline.com/article/2118531/metricsbudgets/metrics-for-corporate-and-physical-security-programs.html

[2]https://mario15494.wordpress.com/category/temas/auditoria-de-la-seguridad-fisica/

[3] Interagency Security Committee (ISC). (2015). Best Practices for Planning and Managing: Physical Security Resources: An Interagency Security Committee Guide. Sitio web: https://www.dhs.gov/sites/default/files/publications/isc-planning-managing-physicalsecurity-resources-dec-2015-508.pdf

[4] Harris, S. (2013). Physical and Environmental Security. In CISSP Exam Guide (6th ed., pp. 427-502). USA McGraw-Hill

[5] Harris, S. (2013). Access Control. In CISSP Exam Guide (6th ed., pp. 97, 98, 157- 277). USA McGraw-Hill;

[6] Harris, S. (2013). Information Security Governance and Risk Management. In CISSP Exam Guide (6th ed., pp. 21-141). USA McGraw-Hill;

[7] http://extintoressecom.mx/blog-secom/tag/triangulo-del-fuego/

[8] http://extintoressecom.mx/blog-ecom/extintores/diferentes-tipos-de-extintores/#comment-2600

[9] http://blog.elinsignia.com/2017/11/04/clases-de-fuegos-y-extintores/

[10] http://www.seguridadsos.com.ar/dvr/

[11] https://www.incibe.es/protege-tu-empresa/que-te interesa/proteccion-puesto-trabajo

[12] NTC-ISO-IEC 27001:2013 Anexo A – A.11 Seguridad física y del entorno.

AUTOR

Manuel Antonio Vera Salgado nació en la ciudad de Bogotá, Colombia. Se graduó como Técnico en electrónica industrial e Ingeniero electrónico en la Escuela Colombiana de Carreras Industriales, actualmente se encuentra culminando la Especialización en Seguridad Informática en la Universidad Piloto de Colombia.

Experiencia en administración de servidores en plataformas Windows y Linux, virtualización con hyper-v y sobre AWS, administrador de plantas telefónicas sobre asterix, UTM fortinet, Sonicwall y Pfsense. Actualmente está liderando un equipo de tecnología en el área de infraestructura y seguridad informática de una compañía financiera.