Ensayo para optar el título del Diplomado BASC

FALENCIAS HUMANAS Y TECNOLOGICAS EN EL CONTROL DE ACCESO EN UNA INSTALACION FISICA

Richard Hernando Losada Muñoz

Tutores

Co ® Luis Alfredo Cabrera Albornoz

Dr. Álvaro Méndez Cortes

Universidad Militar Nueva Granada

Facultad de Relaciones Internacionales Estrategia y Seguridad

Administración de la Seguridad y Salud Ocupacional

Bogotá D.C.,

2013

TABLA DE CONTENIDO

Pág.

1. RESUMEN INICIAL.

La estrategia ideal es que la seguridad contribuya continuamente a mantener la misión-vision y la continuidad de las Organizaciones y para ello deben controlar su punto de acceso a ellas.

El control de accesos en una instalación física nos brinda el control del personal que accede a las instalaciones lo cual es esencial para alcanzar los objetivos relativos de la empresa y tener el control de sus activos. A medida que se abre el acceso a nuevas tecnologías, como la identificación biométrica y la administración remota de datos de seguridad, los métodos de seguridad tradicionales basados en la lectura de tarjetas son reemplazados por sistemas de seguridad que permiten identificar sin lugar a dudas y rastrear la actividad humana dentro de la empresa. Antes de invertir en equipos, los Gerentes deben evaluar cuidadosamente sus necesidades específicas en términos de seguridad y determinar cuáles son las medidas de seguridad más apropiadas y rentables para sus instalaciones. En este ensayo nos lleva a la problemática que existe en las falencias presentadas por el personal y la tecnología que tienen su funcionabilidad en los controles de accesos y se describen los elementos y procedimientos básicos que emplean estos sistemas de seguridad.

Palabras claves: control de acceso, seguridad, deficiencias en el factor humano y de tecnología.

2. INTRODUCCIÒN

Teniendo en cuenta el incremento en las actividades delictivas cometidas por la delincuencia sobre las propiedades, bienes y personas, las sociedades y el ser humano han tenido la necesidad de controlar el acceso a ciertas áreas y lugares; esta necesidad es motivada por el temor que las personas no autorizadas o delincuentes puedan ingresar a sus propiedades a generar pérdidas.

El Control de acceso es una de las herramientas en que se fundamenta la Seguridad, y es así que se puede decir que permite ejercer la medición de los resultados actuales y pasados, en relación con los esperados, en forma total o parcial, con el fin de tomar decisiones oportunas para corregir, mejorar y formular nuevos planes o estrategias.

En sí, el Control de Acceso busca recolectar sistemáticamente los datos para conocer la información oportuna, y bajo un procedimiento previamente establecido, va controlando y evaluando las acciones constantemente con base en los datos suministrados.

Como NORIEGA 2003, enuncia:

Los controles de seguridad se están convirtiendo en un mecanismo para reducir los riesgos, y fortalecer los esquemas de seguridad, las soluciones tecnológicas que existen en el mercado, son de alto costo y limitadas al diseño del programa, y no cubren las necesidades de control específicas de la empresa.

3. DESARROLLO DEL TEMA.

3.1. PLANTEAMIENTO DEL PROBLEMA.

Para poder determinar las falencias en materia de seguridad de una instalación, el primer paso que hay que tener presente en la elaboración de un plan de seguridad es justamente eso: determinar qué personas pueden acceder a la instalación física y evitar que mediante la negligencia, descuido, el soborno y fallas tecnológicas se presente la suplantación de personas autorizadas para poder ingresar a la empresa, es decir las falencias del factor humano y tecnológicas en los controles de accesos en una instalación física.

3.2. CONTENIDO DEL TEMA.

Como VALLEJO 1999, enuncia:

El control de acceso es un sistema que permite controlar el acceso a las áreas y a los recursos en una instalación física dada o un sistema de información. Un sistema del control de acceso, dentro del campo de la seguridad física, se considera generalmente como la segunda capa en la seguridad de una estructura física.

Si vamos a referirnos a la seguridad de una instalación física, lo más probable es que en primer lugar pensemos en sabotaje, espionaje, robo de activos, de información, etc. Si bien la necesidad de protección contra intrusos y el daño intencional que estos podrían causar son obvios, los peligros derivados de la actividad del personal que trabaja en la Organización.

Las personas son esenciales para operar dentro de una empresa pero también hay que tener presente que las personas provocan accidentes y cometen errores, entre los que pueden nombrarse aplicación de procedimientos inadecuados, rotulación incorrecta de equipos, caída de elementos y

derrame de líquidos, errores en el ingreso de comandos, y otros contratiempos de mayor o menor trascendencia. Dado que el error humano es una consecuencia inevitable de la presencia de personas, minimizar y controlar el acceso del personal a las instalaciones es un elemento esencial en la gestión de riesgos, incluso cuando el riesgo de actividades maliciosas es mínimo.

Con el constante surgimiento de nuevos equipos y técnicas, es fácil olvidar que el antiquísimo problema que esas tecnologías tratan de resolver no es técnico ni complejo: mantener a las personas no autorizadas o malintencionadas fuera de espacios que no les corresponden. Y si bien el primer paso determinar cuáles son las áreas seguras de la instalación y establecer reglas de acceso– puede dar origen a un complejo plano con diversos niveles. Los Directivos suelen y deben saber a quién permitir el ingreso a un determinado lugar.

En AMERICAN SOCIETY FOR INDUSTRIAL SECURITY 2003, enuncia:

El primer objetivo de un programa de Seguridad Física es CONTROLAR el ACCESO.

Los controles son considerados como uno de los elementos de un sistema de seguridad.

Los objetivos básicos de un control de acceso son:

- Permitir o denegar la entrada hacia... O la presencia dentro... De un lugar determinado.
- Incrementar o reducir la rata o densidad de movimientos hacia...Desde... O dentro de un lugar dado.

En toda instalación el personal que tiene a su cargo el control de accesos, conforma el primer círculo de seguridad con el apoyo de las barreras físicas y de los elementos electrónicos destinados a impedir, retardar o demorar el acceso de elementos hostiles o de personas no autorizadas, que pudieran vulnerar el sistema, alterándolo parcial o totalmente con su accionar.

❖ Etapas que contempla un Control de Accesos.

En su libro BORGELLO 2009, enuncia:

- Verificación de identidad:

Como su nombre lo indica, tiene por objeto la individualización de la persona que desea ingresar al recinto. La verificación de identidad se realiza por medio de la inspección física del documento de identidad, o en su defecto de la credencial que acredite la calidad funcionaria de la persona, según se trate de un visitante o un empleado de la empresa, respectivamente.

- Autorización/Confirmación: Tiene por finalidad verificar en forma interna si la persona está autorizada para ingresar al recinto. Este paso define si procede el ingreso o no.

- Registro / Acceso: Se procederá a registrar sus datos personales y cargo de la persona que efectuó la autorización/confirmación. Posteriormente otorgarle un distintivo (credencial, pase o tarjeta), que deberá indicar expresamente el área a la cual tiene acceso.

- Verificación de destino: Una vez que el visitante ha ingresado al recinto, se debe efectuar la comprobación de destino. Esta verificación se puede realizar a través de diversos procedimientos, entre ellos:

- Efectuando una llamada desde el Control de Acceso a la oficina de destino.
- Mediante el diligenciamiento de un formulario o volante.

- Salida: Una vez finalizada la visita, la persona devolverá la credencial de acceso, recibiendo su documento personal. Se registrará la hora de salida de la instalación.

- ❖ Tipos de Control de Accesos.

Como afirma CASTRO y LOPEZ 2001:

Existen tres tipos de Control de Accesos. Estos son:

- Controles Manuales: Basan su accionar en personas, ya sean éstos Vigilantes, Guardias de Seguridad, personal administrativo y/o recepcionistas.

Para que este sistema funcione en forma eficiente, se requiere de planificación y adecuada distribución de las zonas restringidas, además de un cabal cumplimiento de los criterios definidos por la empresa para permitir o denegar el acceso a áreas y zonas específicas.

- Controles semimanuales: Utiliza equipos o elementos electromecánicos para apoyar al personal en la evaluación de la solicitud de acceso y en la toma de decisión para permitir o denegar la entrada.

No obstante lo anterior, el rol que juegan las personas que efectúan este control es relevante, debido a que ninguna etapa puede fallar, ya que al ocurrir una falla de un componente o una etapa afectará a las otras y en definitiva, el sistema total fallará.

- Controles automáticos: Son aquellos en los cuales las etapas de verificación y acceso son efectuadas enteramente por equipos o sistemas electrónicos, los cuales están pre programados para tomar decisiones cuando alguien lo requiere.

- ❖ Ventajas de un control de accesos.

Como GLOSARIUM 2003, enuncia:

Implantar un sistema automatizado de control de acceso supone disponer de ciertas ventajas:

- Seguridad de sus instalaciones.
- Ahorro del tiempo dedicado a la gestión.
- Incremento de ingresos.
- Conocimiento en profundidad de cliente y de la instalación: número de accesos, permanencia en la instalación y cobros.
- Modernización de la imagen de sus instalaciones.
- Aumento de competitividad y servicio.

Estas ventajas se convertirán en beneficios y rentabilidad para la empresa.

❖ Características generales.

En su libro BORGELLO 2009, manifiesta:

El control de acceso no solo requiere la capacidad de identificación, sino también asociarlo a la apertura y cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de la Empresa. El servicio de vigilancia es el encargado del control de acceso de una instalación física para cumplir con sus objetivos y controlar el acceso.

Como NORIEGA y RIAÑO 2001, manifiestan:

Un sistema de control de acceso permite monitorear, controlar o restringir el acceso a determinadas áreas. Debido a que cada empresa tiene sus propias normas y/o políticas para restringir el acceso del personal, los cuales son programables y ajustables a dichas necesidades.

En SECURITY MANAGEMENT 2000, enuncia:

Para realizar la selección de usuarios se debe hacer una identificación única del usuario o grupo de usuarios. Hoy en día se conocen tres únicos métodos para identificar personas, son:

- Por las características físicas: biométricos.
- Por un secreto compartido: contraseñas (Passwords).
- Por la posesión de un objeto (software o hardware): Tokens o certificados digitales.

❖ Métodos de identificación.

Como ZUNNANE 2004, enuncia:

La identificación de personas puede clasificarse en tres categorías, cada una de las cuales ofrece mayor confiabilidad que la anterior, pero también exige el uso de equipos más costosos.

- **Lo que la persona tiene.**
- **Lo que la persona conoce.**
- **La identidad de la persona.**

Lo que la persona tiene. Mínima confiabilidad (puede compartirse o ser robado). Es algo que usa o lleva consigo, puede ser algo tan sencillo como una anticuada llave metálica o tan sofisticada como una tarjeta. Lo que la persona tiene es la forma de identificación menos confiable, dado que no existe garantía de que el objeto sea utilizado por la persona indicada; es posible compartirlo y también puede ser robado o extraviarse y ser encontrado por otra persona.

Lo que la persona conoce. Mayor confiabilidad (no puede ser robada, pero puede compartirse o registrarse por escrito).

Es una contraseña, un código o un procedimiento para hacer algo como abrir una cerradura con combinación, realizar una verificación con una lectora de tarjetas o desbloquear el teclado de una computadora. El uso de contraseñas o códigos plantea un dilema de seguridad: si es fácil de recordar, probablemente sea fácil de adivinar; si es difícil de recordar, probablemente sea difícil

de adivinar, aunque también es mayor la posibilidad de que la persona la anote, lo cual reduciría el nivel de seguridad.

La identidad de la persona. Máxima confiabilidad (se basa en un atributo físico único y propio de una persona). La identidad de la persona implica la identificación mediante el reconocimiento de características físicas únicas.

- ❖ Dispositivos para control de acceso.
- Tarjetas. "Lo que la persona tiene".

Como ZUNNANE 2004, enuncia:

En la actualidad se emplean diferentes tipos de tarjetas para el control de acceso, desde las más simples hasta los más sofisticados, que ofrecen diversos grados de rendimiento o dimensiones varias:

- Capacidad de reprogramación.
- Resistencia a la falsificación.
- Tipo de interacción con lectoras de tarjetas: deslizamiento, inserción, apoyo, proximidad.
- Conveniencia: formato físico y modalidad de uso.
- Volumen de datos que incluye.
- Capacidad, costo de tarjetas y costo de lectoras.

Independientemente del nivel de seguridad y confiabilidad que ofrece cada una de estos "objetos" físicos en virtud de la tecnología que emplean, el grado de seguridad que proporcionan se ve limitado por el hecho de que no existe garantía de que los emplee la persona indicada. Por eso, es frecuente combinarlos con otro u otros métodos para confirmación de identidad. Las

tarjetas presentas las desventajas que es relativamente fácil de duplicarlas o leer la información almacenada en ellas, no se pueden reprogramar y fácil duplicación.

- Cerraduras de teclado y de combinación: “Lo que la persona conoce”

Como JOYANES 2000, enuncia:

La seguridad que brindan es limitada ya que toda contraseña puede divulgarse o adivinarse. Presentan un teclado donde los usuarios ingresan un código. En general las cerraduras de teclado aceptan varios códigos, uno por cada usuario; las cerraduras de combinación suelen admitir un solo código, que usan todas las personas.

A las cerraduras de combinación que no se les cambia el código, deberá cambiárseles el teclado en forma periódica si el desgaste de las teclas revela un patrón evidente.

- Biometría: “La identidad de la persona”. Utilizan una característica física del usuario la cual debe ser única en las personas y no cambiar con las circunstancias (estado de ánimo, temperatura ambiente, iluminación, etc...) ni con el tiempo (insensible al envejecimiento). Como ventajas tienen:

– Intransferibles. El atacante no los puede utilizar aunque los conozca. Esta característica es suficiente para considerar el sistema mejor que los de contraseña.
– No necesitan gestión del usuario, como cambiarlos a menudo, recordar frases largas, guardar objetos, etc.
– Sirven tanto para accesos físicos como lógicos.
– Son muy seguros a cualquier ataque.

Actualmente aún tienen desventajas:

- Necesitan electrónica adicional para realizar las lecturas de imágenes y son más caros.
- La tecnología no está muy avanzada.
- Tienen un cierto rechazo del usuario delante de la exposición física a un sensor.
- Hay algún prejuicio moral porque las características físicas de las personas son invariables y hacerlas públicas implica estar fichado para toda la vida.

Como AGUIRRE 19981, enuncia:

En una identificación biométrica se realizan las siguientes fases de captar la imagen o sonido relativo de la persona mediante un sensor y modificar los datos de la imagen o sonido mediante técnicas de tratamiento de señal para extraer los parámetros básicos y únicos del usuario.

En el proceso de comparación biométrica se pueden diferencian dos métodos: identificación y verificación. La identificación consiste en encontrar en una base de datos de parámetros biométricos si los medidos coinciden aproximadamente con algún usuario. La verificación compara directamente los parámetros medidos con los del usuario y se considera el acceso permitido o denegado.

Como ESPIÑERA 2000, manifiesta:

Los sistemas biométricos de la huella, mano, cara, iris y voz, sus desventajas es el deterioro de los registros mismos de la huella, que varía mucho con el tiempo y las condiciones físicas de la persona, debe medir características únicas e invariables con el tiempo y las expresiones de las caras, como la distancia entre los ojos, de la boca a la nariz , el inconveniente es el rechazo social a colocar el ojo delante de un escáner y es muy sensible a factores externos como el ruido de fondo, el estado de ánimo, los atacantes pueden hacer una grabación, o el envejecimiento.

- Guardias de seguridad.

Como DOBSON 2.000, enuncia:

A pesar de todos los avances tecnológicos en el campo de la seguridad física, los expertos concuerdan en que la necesidad de contar con un buen personal de seguridad encabeza la lista de métodos para respaldar y brindar apoyo al control de acceso. Los vigilantes brindan una capacidad de vigilancia con todos los sentidos humanos, además de que pueden reaccionar con movilidad e inteligencia ante eventos sospechosos, inusuales o catastróficos.

El empleo de vigilantes adecuadamente entrenados y supervisados proporciona un elemento valioso de disuasión frente a aquellas personas que puedan planear una intrusión encubierta. Por otra parte, a los guardias se les proporcionarán directrices adecuadas por escrito para asegurarse de que las tareas que les han sido asignadas se llevan a cabo de acuerdo con las necesidades.

Otra problemática disiente del personal de seguridad y de recepcionistas en el control de accesos es:

La seguridad del registro es fundamental, porque si se manipula se tendrá una falsa sensación de seguridad, se convierte en otra problemática de los controles de accesos y como ello se tendrán en cuenta controles para protegerlo de cambios no autorizados y problemas como pueden ser:

- La desactivación del dispositivo.
- Alteraciones al tipo de información registradas.
- La edición o borrado de registros.
- La saturación del soporte del registro, no registrando o regrabando, entre otros aspectos.

4. CONCLUSIONES.

Evaluar y controlar permanentemente el control de accesos en una instalación física es la base para comenzar a integrar la seguridad como una función primordial dentro de cualquier Organización.

Es por eso que debemos de asegurar que cualquier persona que tenga el acceso autorizado a la instalación física de una Organización sea completamente confiable su ingreso y que ninguno de los anillos de seguridad establecidos haya fallado.

Este aspecto cubre uno de los aspectos más importantes y evidentes respecto a la seguridad: la problemática del control de acceso. Las garantías que cubre este dominio son autenticidad y confidencialidad. También es el control base que asegure una buena trazabilidad.

Los permisos de acceso a una instalación se otorgarán de modo que los usuarios tengan acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones.

Es ahí donde el factor humano juega un papel determinante para que los procedimientos y perfiles de accesos establecidos se apliquen y cumplan para lo cual se han establecido.

Las credenciales de acceso de cada usuario serán personales e intransferibles. Toda persona registrada que disponga de credenciales de acceso será responsable de mantener su confidencialidad y asegurar su correcto uso. Se establecerán los mecanismos necesarios en los sistemas para impedir la visualización de las credenciales por parte de terceras personas.

Debido a que una protección efectiva necesita la cooperación de los usuarios autorizados, los usuarios deben ser conscientes de sus responsabilidades en el mantenimiento de la efectividad de

las medidas de control de acceso, en particular respecto al uso de contraseñas y a la seguridad del material puesto a su disposición.

Al igual se debe de realizar una verificación y seguimiento al desarrollo de las actividades ejecutadas por el personal que ejerce la función de desplegar registro sobre los controles de accesos en el proceso de identificación, registro, autenticación y autorización, para evitar que se presenten falencias en el factor humano que convergen y llegan afectar el área de seguridad.

Los usuarios de los controles en una estructura física deben de ser conscientes de la importancia de la seguridad en los sistemas de control de accesos. La seguridad eficaz depende, en parte, de que los usuarios sepan lo que se espera de ellos y cuáles son sus responsabilidades, comprometiéndose con las mismas. Éstos deben conocer los motivos de las medidas de seguridad establecidas y también las consecuencias de violar la seguridad.

Teniendo en cuenta las preocupaciones actuales por la seguridad, los sistemas de control de accesos parecieran ser inevitables. Pero de hecho sigue habiendo resistencia considerable a ellos. En conclusión, los controles de acceso son utilizados y empleados por las personas como un certificado de identidad, ya que por estos nos permite determinar en cada persona su ubicación en una instalación física, y su campo de acción se está expandiendo en los sistemas de seguridad en diferentes áreas.

5. BIBLIOGRAFIA.

AGUIRRE MARTÍNEZ, Eduardo. Seguridad y Protección: a personas, empresas y vehículos, México: Trillas, 1998.

AMERICAN SOCIETY FOR INDUSTRIAL SECURITY. Conferencia de Seguridad Física 2003.

BORGELLO, Cristian F. "Seguridad Informática: sus implicancias e implementación" Cáp. 2, Seguridad Física, Pág.10, 2009.

CASTRO, Octavio y LOPEZ, Luis Enrique. National & International Load Protection System (SPC) Physical Security Departament. Colgate Palmolive. Cali, 2001.

DOBSON, Rick. Programando con Access. 2.000.

ESPIÑERA, Sheldon y Asociados. Optimización de los controles de Acceso mediante tecnología complementaria. Pc-news.com. 2000.

GLOSARIUM. Diccionario Informático. (on line) España, 2003. www.glosarium.com.

JOYANES, Luis. Fundamentos Básicos de Programación. Mc Graw Hill. 2000.

MONOGRAFIAS, Trabajo No. 5. (on line) México. 2002.

NORIEGA PERALTA, Eduardo y RIAÑO Julia Aurora. Descubra al Delincuente. Bogotá, 2001.

SUZANNE, Niles Wes Kussmaul, Quiet Enjoyment, Massachusetts, 2004.

VALLEJO ROSERO, Silvio. Prevención y Control de Pérdidas y Daños., Bogotá: Asesorías de seguridad Privada, 1999.