POLITICAS DE SEGURIDAD INFORMATICA COMO HERRAMIENTA PARA LA PRESERVACION E INTEGRIDAD DE LA INFORMACION EN LAS EMPRESAS DE SEGURIDAD PRIVADA EN BOGOTA

Anderson David Cáceres Goyeneche

Universidad Militar Nueva Granada
Relaciones Internacionales Estrategia y Seguridad
Administración de la Seguridad y Salud Ocupacional
Bogotá
2015

POLITICAS DE SEGURIDAD INFORMATICA COMO HERRAMIENTA PARA LA PRESERVACION E INTEGRIDAD DE LA INFORMACION EN LAS EMPRESAS DE SEGURIDAD PRIVADA EN BOGOTA

Anderson David Cáceres Goyeneche

Trabajo de Grado

Álvaro Marroquín Villadiego (Director de ensayo)

Universidad Militar Nueva Granada
Relaciones Internacionales Estrategia y Seguridad
Administración de la Seguridad y Salud Ocupacional
Bogotá
2015

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

CONTENIDO

LISTA DE ANEXOS

RESUMEN

Estamos en una época en la cual el uso de la información es una prioridad ya que es un activo que tiene mucho valor, y debido a esto las empresas deben darle un uso adecuado y tener una estructura planteada, que permita que información Confidencial mantenga su integridad dentro de una empresa, ya sea una información de un gran valor o que no tenga tanto impacto dentro de la misma.

El hecho es que una organización presta un servicio o vende un producto y en todos sus niveles jerárquicos, maneja cierta información, de modo que para el buen funcionamiento de una empresa, es de vital importancia el cuidado de la información y en particular en el sector de la seguridad privada en Bogotá ,se torna importante el manejo que se le debe dar, por qué el servicio que se presta incluye no solo la empresa de seguridad oferente a la actividad realizada, sino varias empresas a las cuales se les presta un servicio; adicionalmente se vende SEGURIDAD que incluye la información suministrada por las empresas. Ahora bien en Bogotá hay más de 800 empresas de seguridad privada. La ISO (la organización internacional para la estandarización) crea una norma llamada la ISO 27001, mediante la cual suministra unos lineamiento para preservar la integridad de la información y entre ellos se encuentra la definición de unas políticas de seguridad informática ,en las cuales suministra herramientas que puedan ayudar a proporcionar dirección gerencial y apoyo a la seguridad de la información en congruencia con lo establecido legalmente con respecto a los requerimientos comerciales, leyes y regulaciones relevantes. Así surge un interrogante ¿están las empresas de seguridad privada en Bogotá implementando las políticas de seguridad informática? Y aún más importante ¿están haciendo uso de ellas y se están revisando periódicamente para su mejoramiento? , por ell

o miraremos como plantea la ISO 27001, las políticas de seguridad de la informátic a y como pueden ser usadas como una excelente opción para la preservación e int egridad de la información en las empresas de seguridad privada en Bogotá, analiz ando los lineamientos planteados por la norma, mirando estadísticas acerca de la i nformación y planteamientos de otros autores para que de esta manera se tome co nciencia de la importancia de no solo establecerlas, sino aplicarlas.

Palabras clave: Seguridad Informática, ISO 27001, Prevención, Integridad de la inf ormación.

1. INTRODUCCIÓN

La seguridad ha estado presente siempre y es una necesidad básica de cualquier p ersona ¿y que es seguridad? Es un estado de bienestar que disfruta y percibe el s er humano, de igual forma una familia, una sociedad y una empresa. La seguridad tiene varios campos entre ellos la Seguridad Informática y hoy en día la tecnología ha llegado a tener tanto impacto en el mundo que es fundamental para el uso diari o de cada persona. En 1973 se crea el primer celular con un costo elevado y pocas personas hacían uso de él, en la actualidad es normal que un niño lo posea y en e sta época existen teléfonos inteligentes que prestan un servicio de comunicación p or voz, pero adicionalmente permiten hacerlo por medio de internet y prestan much as aplicaciones adicionales, haciendo de un teléfono, un computador un activo con mucho valor no solo por el costo que pueda tener, sino por la información que pue da estar almacenada en él.

En el ámbito laboral de una empresa de seguridad privada el uso y manejo de la in formación debe ser prioritario y cuidadoso y debe ser de gran impacto dentro de la misma que de llegar una información confidencial a malas manos, puede causar su quiebra o daños a las empresas que les presta un servicio.

En la actualidad en Bogotá existen múltiples empresas de seguridad privada y hac e algún tiempo tuve la oportunidad de laborar en una de ellas. Aprendiendo y vivie ndo experiencias enriquecedoras, comprendí el valor que tiene la información, sin e mbargo, en el proceso que laboré tuve acceso a múltiple información confidencial. Estudiaba en las noches en la universidad y de acuerdo a la educación recibida y l a experiencia vivida dentro de ella, es de gran importancia comprender cuando se observan planteamientos dados en el área teórica y salir a un mercado en el cual h ay muchas necesidades de mejora entre ellas una cultura de prevención. Es por es o que surgen interrogantes con respecto al cuidado de la información ¿existe una p olítica de seguridad informática en las empresas de seguridad privada en Bogotá? Y aún más importante ¿Están siendo aplicadas estas políticas dentro de la empres

a? Ciertamente en siete meses que laboré, en ningún momento tuve conocimiento si la había y mucho menos que se aplicara, es por ello que una información mal uti lizada puede causar gran impacto en términos de daños dentro de la misma y es cl ave saber cómo se pueden usar las políticas de seguridad de la información como una excelente herramienta para la preservación e integridad de este tópico, de acu erdo a los lineamientos planteados por la ISO 27001 en las empresas de seguridad privada en Bogotá.

2 DESARROLLO

Hace un siglo no existía la tecnología con la que hoy contamos; el proceso evolutiv o que ha tenido la misma, ha causado un cambio global en el mundo y siempre ha sido importante la información; antes había pergaminos sagrados, en esta época h ay dispositivos de almacenamientos de información, denominadas memorias USB, cuentas bancarias, teléfonos inteligentes e internet; todos estos con información al macenada. La tecnología ha venido avanzando rápidamente a tal punto que a un c lic se encuentra todo tipo de información de modo que todo es más fácil de obtener por ello tal vez dijo Albert Einstein ‘‘Temo el día en que la tecnología sobrepase nu estra humanidad el mundo tendrá una generación de idiotas’’[1] usamos los computa dores ,teléfonos y tablet, para buscar todo tipo de información, para comunicarnos con otra persona en cualquier lugar del mundo, para hacer negocios, para enviar in formación, para hacer transacciones, se hace todo más fácil, pero no usamos de fo rma adecuada todos estos medios , incluso estamos en la era del internet rápido y las mentes lentas, no necesitamos pensar ,tomar conciencia, buscar alternativas y es por eso que hoy en día en Bogotá no hay cultura preventiva, se espera que suc eda un daño y se trata de corregir si es posible hacerlo, si se pierde información va liosa para una empresa , se intenta recuperar si hay la forma de hacerlo.

José Martí escribió ‘’ver después no vale, lo que vale es ver antes y estar preparado’’[2] y entendiendo un poco esta frase, el prevenir lo han hecho desde mucho tiempo atrás, en las civilizaciones antiguas. Para anticipar el paso de personas no autorizadas y evitar daños, se construyeron castillos medievales; en la construcción de la Gran Muralla China se hizo de una altura de seis a siete metros de alto para evitar el paso del enemigo y es interesante observar como desde mucho tiempo atrás existe el concepto de la prevención, por lo cual invito a recordar este término que según el diccionario de la Real Academia de la Española es la

[1]http://www.proverbia.net/citasautor.asp?autor=327,Albert Einstein

[2] http://www.proverbia.net/citasautor.asp?autor=641, José Martí

“preparación y disposición que se hace anticipadamente para evitar un riesgo o ejecutar algo”[3], del tal modo que llevado al aspecto informático se trata de saber si puede ocurrir un daño, si se hurta, pierde o extravía la información y que impacto puede traer a la empresa, por consiguiente, observar que puede suceder si se pierde cierta información y tomar acción para evitar que pueda materializarse lo previsto. Esto funciona para todas las empresas en el mundo, pero hay un sector que busca prevenir como prioridad y son las empresas de seguridad privada, por ello se generan interrogantes en el ámbito de la seguridad privada en Bogotá ¿está siendo la información que manejan estas empresas protegida? Así entramos en conceptos relativos al tema, uno es el de la Seguridad Privada , el Estatuto de Vigilancia y Seguridad Privada lo define como ‘’las actividades que en forma remunerada o en benefició de una organización pública o privada, desarrollan las personas naturales o jurídicas, tendientes a prevenir o detener perturbaciones a la seguridad y tranquilidad individual en lo relacionado con la vida y los bienes propios o de terceros y la fabricación , instalación ,comercialización y utilización de equipos para vigilancia y seguridad privada, blindajes y transportes con el mismo fin’’[4]. Hoy en día es un bien que se compra y se vende ,de modo que la seguridad privada ha pasado a ser cada vez más un estilo de vida y sus pilares más fundamentales son inicialmente la prevención ,ver con anticipación. Conocer, conjeturar por algunas señales o indicios lo que ha de suceder, disuadir; por medio de diferentes mecanismos y herramientas de seguridad lograr que un agente dañino no logre realizar su objetivo, controlar; en el momento en que se materialice un riesgo, lograr tomar acción ante él y controlarlo, proteger; evitar que un agente externo logre causar un daño y vigilar; es estar constantemente observando el medio que se quiere proteger a fin de que no se presentan amenazas. Una seguridad integral en donde la seguridad no se desarrolle de manera fragmentada, sino que la estructura organizacional completa sea integral, que se analice en conjunto, se determinen los

[3] Real academia española, conceptos, prevención

[4] Estatuto de vigilancia y seguridad privada, Dec 356 de 1994

riesgos y se actue ante las posibles pérdidas o riesgos de daño ,amenazas, peligros, ataques ,vulnerabilidades e incidentes y algo clave es que se observa todo esto desde el punto de vista de seguridad física, de bienes o de personas y dentro del entorno laboral y siendo la magnitud del servicio prestado por estas empresas tan grande ¿es importante cuidar la información que es suministrada a ellos de posibles, riesgos, amenazas ,peligros, ataques, daños, vulnerabilidades e incidentes? Por supuesto que es de vital importancia la confidencialidad de todos los recursos con los que cuentan y se usan para prestar los diferentes servicios de seguridad a las empresas, por eso la seguridad de la información debe ser siempre una prioridad.

La información es un recurso que, como el resto de los activos, tiene valor para una organización y por consiguiente debe ser debidamente protegida. La seguridad de la información protege ésta de una amplia gama de amenazas, a fin de garantizar la continuidad del negocio, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades.

La información puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por un medio electrónico, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada, y con lo anteriormente mencionado, una de las principales fuentes de información es la que se encuentra almacenada en medios electrónicos y de hecho es una de las cuales más debe ser custodiada. Las diferentes organizaciones tienen en su poder un producto, un servicio o una estrategia de cómo llevar al mercado la actividad que realizan y por consiguiente tener un valor agregado; ello lo suministra cierta información, ya sea un método de trabajo, una receta de un producto, herramientas como publicidad, innovación y dentro de todos estos factores existe algo en común y es que esto puede ser vulnerado.

Segu-info que es la comunidad hispana más grande sobre seguridad de la información en agosto de 2013 expresa ‘’los ataques informáticos pueden causar graves pérdidas de información si no son identificados y controlados a tiempo y muestra unas estadísticas interesantes expuestas por McAfee que revelan cifras que continúan alarmando a las organizaciones respecto a la seguridad de su información. De acuerdo con los datos reportados en Needle in a data risk: the rise of big security data, solo el 35% de 500 compañías entrevistadas alrededor del mundo, están en capacidad de identificar y controlar una filtración en los primeros minutos y es importante resaltar que es en empresas norteamericanas, británicas, alemanas y australianas cuyo nivel tecnológico es de un avance amplio. Un informe The Economic Impact of Cybercrime and Cyber Espionage, publicado por el Center for Strategic and International Studies (CSIS), confirma pérdidas por cien millones de dólares anuales por delitos informáticos y dice que los ataque a las empresas y los consumidores son cada vez más comunes y la economía sufre con los delincuentes informáticos que roban identidades, propiedad intelectual, secretos comerciales y cualquier otra cosas que puedan tener en sus manos , solo un porcentaje mínimo de las empresas logra actuar cuando hay una infiltración por medios electrónicos y debido a esto se dan pérdidas tan grandes en cuestión financiera’’[5] entonces se deduce lo importante de una cultura preventiva mediante la cual se custodie la información. Lograr que estas estadísticas mejoren no es difícil, se necesitan unos parámetros que establezcan cuidados adecuados de la información dentro de una empresa y ponerlo en práctica, de modo tal que eso ayudaría a disminuir cifras tan alarmantes como la anteriormente observada. Es claro que no hay seguridad total, pero si las pérdidas anuales se reducen en un porcentaje significativo, las empresas tendrían más solidez y mejor crecimiento.

[5] https://seguinfo.wordpress.com/category/estadisticas/, 2013

Cada vez se presentan más pérdidas y los medios constantemente se habla más de la problemática; revisemos estadísticas del País porque así como grandes países son constantemente víctimas de ataques a su información, en Colombia también se presentan casos. El 15 de octubre de 2014 el Estado socializa unas recomendaciones de expertos en Seguridad de la Información en este informe la Viceministra de Tecnologías y Sistemas de la Información, María Isabel Mejía Jaramillo resaltó ‘’la importancia de adoptar en Colombia, los más altos estándares de calidad en materia de protección de datos debido al crecimiento acelerado de este tipo de delitos en el mundo. En 9 meses en el 2014, se presentaron 121 ataques cibernéticos en el país. Por lo tanto se exigirá a las empresas una certificación en capacidades de seguridad’’[6] .Lo cierto es que se tomen medidas preventivas o no lo ataques seguirán surgiendo, lo delincuentes no descansan, ¿pero cómo lograr una integridad de la información si se está expuesto todo el tiempo a riesgos informáticos? Buscamos lograr una cultura preventiva de varias maneras como capacitaciones, normas, reglas y lo importante es que no se ha llegado a entender la magnitud de lo que puede suceder con una información filtrada. En Colombia en muchas empresas se presentan hurtos de información, de dinero y daños informáticos. En contadas ocasiones por proteger el *goodwill* (buen nombre), las empresas prefieren mantener oculta la información de que fueron víctimas de un ataque como hurto de información y en la mayoría de las organizaciones se opta por no denunciar porque entre otras razones, no les conviene publicar lo que podría revelar debilidades de sus sistemas y además implicaría una revisión de todos sus recursos de seguridad y las estadísticas aumentarían, sin embargo hay algo concreto, no se protege la información dentro de una empresa, en diversas ocasiones se presenta el daño y la pérdida, se toma medidas correctivas, pero no se muestra lo ocurrido a las empresas y no se ve la magnitud de la problemática que está presente en cifras reales.

[6] El Estado Colombiano socializa recomendaciones de expertos en Seguridad de la Información, María Mejía, 2014

En un artículo de la Cámara Colombiana de Informática y Telecomunicaciones, entidades expertas en seguridad informática en Colombia “encuentran que el robo de información, fraudes bancarios, secretos empresariales y otro tipo de delitos no obedecen a la falta de programas y herramientas para proteger los equipos, sino en la confiabilidad que tienen los usuarios para navegar y manejar informaciones privadas por la red. La desconfianza para hablarle a un desconocido o la precaución para cruzar una calle, deben ser las mismas medidas que los usuarios deben tener día a día para acceder a portales, abrir correos, manejar memorias y manipular información privada en computadores ajenos’’[7] no obstante, si no se toman medidas al respecto, por más herramientas que existan para proteger la información seguirán presentándose delitos. Los especialistas de la Cámara Colombiana de Informática expresan que los delitos más crecientes en la región y en Colombia van dirigidos específicamente a los usuarios de la banca en línea, delitos que no son en contra del banco sino de quienes usan el banco. Delitos que permiten hurtar información financiera para cometer fraudes, blanquear cuentas, hacer transferencias a cuentas ficticias que luego son desocupadas a través de un cajero. Estos casos han tenido un bajo perfil y poca publicidad porque se crearía un ambiente de paranoia de la banca en línea que afectaría él buen nombre de las corporaciones bancarias; sin embargo, es un delito que está creciendo, principalmente por la falta de conciencia de los riesgos que conlleva el mal uso de la Internet.

El otro objetivo es el hurto de información de tipo corporativo. En este se sustrae información de un competidor para beneficiar otro y se obtienen beneficios por ello en el mercado negro. Pero entre las anteriores modalidades delictivas es de destacar el hurto de claves para conocer información de cuentas de correo de personas cercanas, como el esposo o el novio.

[7] Cámara Colombiana de Informática y Telecomunicaciones, delitos informáticos,2014

Los hechos más frecuentes relacionados con el hurto de la información son los que se hacen mediante los servicios informáticos. De esta manera se presentan problemas de difamación, hurto de información privada para estafas o de información financiera, amenazas y espionaje industrial. En Colombia se han presentado casos donde el propietario pierde el control de su página web hasta el punto de no poderle hacer modificaciones, hasta el momento que le llega un correo electrónico informándole que se apoderaron de su página web y que debe cancelar cierta suma de dinero para devolverle la administración del sitio.

Si el mayor inconveniente está en la facilidad de entrar a la internet y manejar información privada por este medio, una buena alternativa para preservar y mantener la integridad de la información está en establecer Políticas de seguridad informática. Segu-info que es la comunidad hispana más grande sobre seguridad de la información, ayuda a mostrar la importancia de ellas. Hoy es imposible hablar de un sistema con un 100% de seguridad, la seguridad total no es posible lograrla. Por eso las empresas, en general, asumen riesgos: deben optar entre perder un negocio o arriesgarse a ser hackeadas.

La cuestión es que, en algunas organizaciones puntuales, tener un sistema de seguridad informática es una aspiración muy limitada lo cual les impediría hacer más negocios. Si un Hacker quiere gastar cien mil dólares en equipos para descifrar una encriptación, lo puede hacer porque es imposible controlarlo. Y tratar de evitarlo podría representar millones de pesos.

La solución entonces, sería enlazar todo el panorama de seguridad, en lo que hace a plataformas, procedimientos y estrategias. De esta manera se puede controlar todo un conjunto de vulnerabilidades, aunque no se logre la seguridad total. Y esto significa que es un gran avance que puede ayudar mucho a la seguridad informática.

En este sentido, las Políticas de Seguridad Informática (PSI), surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos. Estas permiten a las compañías, desarrollarse y mantenerse en su sector de negocios, siendo entonces las políticas de seguridad informática una forma de comunicarse con el personal al ser un canal que permite actuar, con respecto a los servicios y recursos informáticos dentro de la empresa. De este modo se establecen procedimientos y reglas que pueden regular la forma en que una organización protege, implementa y previene los diferentes daños que se presentan.

‘’El MINTIC (Ministerio de Tecnologías de la Información y las Comunicaciones) en el 2013 hace una campaña llamada “sensibilización seguridad de la información” que tiene como objetivos principales son “realizar las gestiones necesarias con el Ministerio de Educación Nacional y el SENA ,para la generación de un plan de capacitación para el sector privado en temas de ciberseguridad y de seguridad de la información; formular lineamientos, sensibilizar, concientizar; asesorar y acompañar a las entidades en la implantación de un modelo estructurado que permita cuidar la información”[8]. Según esta campaña se muestra una estadística en la cual de veintitrés países, Colombia es la que más recibe ataques informático con un total de mil noventa y ocho ataques diarios ,con una diferencia porcentual de más de (500%) quinientos porciento de cantidad de ataques, y es debido a que en las empresas no hay políticas o directrices de prevención, de modo que en esta campaña de sensibilización se describe una estrategia de trabajo que se detalla y es coherente con los lineamientos del estándar NTC:ISO/IEC 27001:2005.En la norma uno de los aspectos importantes de su implementación es la política de seguridad de la información para la entidad e implementar la misma la cual aporta unos parámetros que ayudan a establecerlas de una forma bien estructurada y

[8] Sensibilización seguridad de la información,MinTic,2013

fomenta en sus usuarios para que enfaticen en la necesidad de establecer políticas de seguridad informática. Este estándar internacional adopta el modelo del proceso planear-hacer-chequear-actuar (PHCA) el cual se puede aplicar a todos los procesos del sistema de seguridad de la información (SGSI), que incluye la política de seguridad informática.

El modelo que usa la norma, aplicado a las políticas de seguridad de la información es (PHCA): Planear las políticas de seguridad de la información, en este aspecto se establecen las mismas, dando estructura a los parámetros que plantea la norma; Hacer es implementarlas dentro de la organización y es adecuado tener en cuenta que la implementación incluye el conocimiento de las mismas por todos los trabajadores de la empresa; Chequear se ejecuta después de cierto tiempo cuando se debe realizar una revisión periódica para constatar si suceden cambios significativos dentro de la organización; y Actuar es darle mejora continua a las políticas para que cumplan el fin para el cual fueron elaboradas.

La norma suministra unos lineamientos mediante los cuales establece que lo primordial que debe realizar una organización es definir una política de seguridad de la información en términos de las características del negocio, la organización, su ubicación, activos y tecnología y generar unos parámetros que debe incluir esta política: un marco referencial para establecer sus objetivos y definir un sentido de dirección general y principios para la acción con relación a la seguridad de la información, con lo cual permite dar trasparencia de lo que se busca con la política de seguridad informática y define qué clase de información se trata de proteger; hay que tomar en cuenta los requerimientos comerciales y legales o reguladores y las obligaciones de la seguridad contractual, para estar acorde con lo establecido y cumplir con las obligaciones de ley; esto debe estar alineado (acorde) con el contexto de la gestión del riesgo estratégico de la organización en el cual se dará el establecimiento y mantenimiento del Sistema de Gestión de Seguridad de la

Información(SGSI), de tal forma que se pueda partir de las políticas para entender el riesgo que puede tener la empresa y que busca evitar por medio del modelo planteado por la norma ISO 27001 y establecer el criterio con el que se evaluará el riesgo, para tener unidad de medida en la forma en que se le realizará evaluación a los mismos, contando con la aprobación de la gerencia para proceder a su implementación.

Adicionalmente al implementar las políticas de seguridad informática en una empresa, se requiere disposición de cada uno de los miembros de la organización para lograr una visión conjunta de lo que se considera importante y en unión con los lineamientos de la norma, definir políticas que deben tener un alcance, que incluyan facilidades, sistemas y el personal involucrado . Este procedimiento debe mostrar las espectativas de estas políticas, en la que se defina claramente la importancia de la información como un activo prioritario que es de ayuda fundamental para el crecimiento de la empresa. Unos objetivos y una descripción clara de los elementos que se involucran en su definición, son importantes para llevar claridad de lo que se desea específicamente, así como responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización, para alcanzar unidad y que cada funcionario adopte sentido de pertenencia frente a estas políticas y su cumplimiento; definir infracciones a la ley y consecuencias de incumplir con la regulación en seguridad informática, lo cual se plantea para dar soporte al importante aporte que se pretende con este ensayo y lograr un compromiso más amplio para el cumplimiento de las políticas de Seguridad de la Información y responsabilidades definidas y concretas a los usuarios que tienen acceso a determinada información sensible, concientizándolos acerca de la forma adecuada de manejar recursos dados por la empresa que usan como herramienta para desempeñar diferentes funciones laborales.

En la norma hay puntos claves para el control de las políticas de seguridad de la información, los cuales incluyen definir un objetivo en el cual se pueda dar apoyo a

la seguridad de la información en concordancia con las disposiciones legales vigentes, además, al documentar esta política, la Gerencia lo debe aprobar mediante un documento el cual debe ser socializado y publicado ante todos los empleados y entidades externas relevantes y finalmente, se deben realizar revisiones de la política regularmente a intervalos planeados o de ocurrir algún cambio significativo. Sin embargo, cuando se quieren controlar las políticas de seguridad de la información en una organización, hay que tener en cuenta que la gestión de seguridad puede tornarse compleja, no por razones técnicas y si por falta de estructura organizacional.

Si se reconoce que en la actualidad la información de las Empresas de Seguridad Privada, son activos valiosos y a medida que los sistemas de información buscan apoyar los procesos de confidencialidad de información crítica; se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos y recursos aportados a los empleados. Las Empresas entre ellas las de Seguridad Privada, se enfrentan a muchos riesgos entre ellos el fraude por computadora, espionaje con fines delictivos, sabotaje de la información, vandalismo y hurto de información. Las posibilidades que se materialice el riesgo y surja un daño con pérdidas de información por causa de un código malicioso o ataques de externos, de hackers, crackers entre otros; se hacen cada vez más comunes.

Siendo tan importante la información confidencial que manejan las empresas, en Bogotá es importante tener una cultura preventiva y en las Empresas de Seguridad Privada debe ser una prioridad. Estas organizaciones tienen un campo de desarrollo amplio pues prestan un servicio muy importante a la sociedad entre ellos enumeramos algunos tales como servicios de vigilancia y seguridad privada con armas de fuego o con otros medios como caninos, tecnológicos, servicios de vigilancia y seguridad a empresas públicas o privadas; servicios de trasporte de valores; servicios de asesoría e investigación en seguridad y por ello es que

manteniendo un buen uso de los recursos que brindan estas empresas, se puede preservar y mantener la integridad de la información.

Por medio de la implementación de políticas de seguridad informática en las Empresas de Seguridad Privada en Bogotá, guiados por los lineamientos de la ISO 27001, se pueden prevenir riesgos que afecten la continuidad del negocio. Si observamos con detenimiento, es de deducir la gran ayuda y soporte que suministran las políticas de seguridad a este tipo de empresas; si bien es cierto, la norma ISO 27001 suministra unos parámetros para implementarlas, cualquier Empresa de Seguridad Privada tiene claro que el servicio prestado es de índole privado, por consiguiente al identificar las características del negocio, encontramos que gran parte de la información que se haya en la empresa es de carácter confidencial, de modo que los activos informáticos que poseen son muy valiosos y de esta manera, en el momento de adoptar un marco referencial, se debe tener en cuenta el alcance de las políticas, para que se logren obtener todas las áreas que componen la entidad, sus recursos, los procesos que se manejan internamente, y dar inicio a los objetivos de proteger, preservar y cuidar la información junto con las tecnologías utilizadas dentro de los procesos laborales , contra riesgos, amenazas sean internas o externas ,con el fin de asegurar la confidencialidad del servicio prestado y la integridad de la información. Mantener la política de seguridad de la información vigente operando y actualizada dentro del marco de los riesgos globales permiten asegurar su eficacia y permanencia constante, la cual debe tener en cuenta los requerimientos comerciales y legales, incluyendo los del servicio prestado de seguridad privada, asumiendo y generando responsabilidades para cada persona de la empresa; verbigracia, el Gerente de la Empresa de Seguridad Privada es el encargado de estar revisando contantemente las políticas de seguridad de la información y estas a su vez deben estar alineadas con los procedimientos y estrategias para la gestión del riesgo, y debe establecer el criterio con el que se evaluará el riesgo y si lo hay de hurto informático, podría definir una

estrategia de alto, medio o bajo y unos parámetro en caso de que hallan riesgos aceptables. Finalmente, el gerente de la empresa de seguridad privada debe dar la aprobación de las políticas y hacer que sean conocidas por todos los empleados. Algunas de las políticas de seguridad informática más encontradas en las empresas son:

- Realizar respaldo de la información cada día, semana o mes.
- No descargar música, películas u otros archivos ilegales.
- No abrir documentos adjuntos o hacer clic en enlaces de mensajes no solicitados.
- No visitar sitios web pornográficos o de contenido ilícito.
- No proporcionar datos personales a desconocidos por teléfono o email.
- No utilizar la misma contraseña en diferentes páginas web y compartirlas.
- Identificar y priorizar los recursos informáticos de la empresa.
- Establecer condiciones de uso del correo electrónico y navegación.
- Disponer de un plan de contingencia que contemple copias de resguardo, autenticación de usuarios, integridad de datos, confidencialidad de la información almacenada y control de acceso.
- Actualizar de manera constante y observar las normas laborales.

- Educar y capacitar constantemente en las políticas de la empresa.

Estas políticas generan punto de partida para poder plantear las de seguridad informáticas en las Empresas de Seguridad Privada en Bogotá, y observar la importancia que trae consigo interrogantes acerca de cómo se está usando actualmente la información dentro de una organización; adicionalmente integrar el uso del internet de forma adecuada pues es posible navegar seguro en él. Es posible además agregar recomendaciones como disponer de dispositivos siempre actualizados, evitar la consulta de correos spam, renovar constantemente el antivirus, evitar ingresar a páginas donde ofrezcan premios inesperados, ingresar siempre al sector financiero a través de sus páginas web y no mediante re direccionamiento desde otras páginas, y estar observando que al escribir la clave, la página no retorne al inicio. Esto permitirá dentro de una Empresa de Seguridad Privada dejar el desconocimiento, la falsa sensación de seguridad y abstenerse de compartir información abiertamente, lo cual permitirá mantener el contenido de los activos de información completos y como hecho más importante, generará en la cultura de todos los empleados, el valor de preservar y custodiar la información.

Fomentando una conciencia de prevención en el aspecto informático, encontré que las políticas de seguridad informática, representan un excelente medio para operar el uso de los recursos informáticos en una empresa, de manera estructurada con los lineamientos que aporta la ISO 27001 para lograr de manera más fluida la implementación de políticas de seguridad de la información de manera tal que se podrá detectar con más claridad, la falta de las mismas en las Empresas de Seguridad Privada en Bogotá, por eso siendo el servicio prestado por estas empresas, de carácter privado, deben adoptarlas y aplicarlas en la organización. Esto les dará una ventaja muy grande sobre quienes la información es como un juego y tendrán un valor agregado en el mercado, por qué su confidencialidad será más efectiva y por tanto genera mayor sensación de seguridad entablar relación

comercial con una organización que custodie con el debido celo uno los recursos más importante que tiene una empresa, la información, porque quizás, elementos tecnológicos ,infraestructura y bienes materiales, se pueden obtener cuantas veces se desee pero los años de experiencia y secretos empresariales no se pueden obtener con la misma facilidad. De este modo las Políticas de Seguridad Informática se constituyen como una excelente herramienta para la preservación e integridad de la Información.

3 CONCLUSIONES

1. La falta de cultura preventiva en seguridad informatica ha causado que Colombia sea uno de los países que más ataques a la información tiene, en razón al uso indebido de las tecnologías dentro de las empresas, por no tener estructurados lineamientos que ayuden a prevenir el mal uso de los recursos informáticos.

2. Las empresas que son víctimas de daño a la integridad de su información, deben hacer una reestructuración para replantear lo que se realiza con la información para establecer políticas de seguridad de la misma, según los lineamientos de la ISO 27001.

3. La ISO 27001 aporta lineamientos claros y sencillos para la implementación de la política de seguridad informática en las Empresas de Seguridad Privada en Bogotá y suministra un punto de partida, haciendo más fácil su establecimiento y adopción para que cualquier empresa pueda tenerla, generando de manera simultánea, una cultura preventiva por medio de las mismas.

4. Todos los empleados en una organización deben entender y asimilar que al hacer uso inadecuado de los recursos informáticos en actividades tales como navegar con fines personales, usar memorias USB para fines personales, descargar programas ilegales, descargar música ilegal, ingresar a páginas pornográficas y el uso de correo para fines personales; puede llevar a la empresa a afrontar daños a su información valiosa y confidencial.

5. A la hora de implementar una política de seguridad informática en una empresa, debe haber una cooperación de toda la organización, para que haya una visión conjunta, en donde todos los integrantes ayuden al cumplimiento y se logre llegar al objetivo que es preservar y mantener la integridad de la info

rmación.

6. Los servicios que prestan las Empresas de Seguridad Privada, van ligados a la información que les suministran, siendo esto prioritario cuando de custo diar la información se trate.

7. Al establecer políticas de seguridad informática, en los servicios de segurid ad privada, se logra obtener mayor confidencialidad con sus clientes y por l o tanto se puede prestar un servicio de mayor calidad.

BIBLIOGRAFÍA

Andrade, Francisco (2015) Conceptos Generales y Fundamentos de Seguridad

Decreto (1994) Estatuto de vigilancia y Seguridad Privada. Decretó 356

Andrade, Francisco (2015) Pilares de la Seguridad

Collazos, Manuel (2014) La nueva versión ISO 27001:2013 un cambio en la integración de los sistemas de seguridad, Seguridad de la información.

Segu-Info, (2013).Solo el 35% de las organizaciones detecta filtraciones en los primeros minutos, Estadísticas. Recuperado de https://seguinfo.wordpress.com/category/estadisticas/

Segu-Info, (2013).Estudio confirma pérdidas US$100 mil millones anuales por delitos informáticos, Estadísticas. Recuperado de https://seguinfo.wordpress.com/category/estadisticas/

Mejía, María (2014) El estado Colombiano Socializa Recomendaciones de expertos en seguridad de la información, Estadísticas. Recuperado de http://www.mintic.gov.co/portal/604/w3-article-7319.html

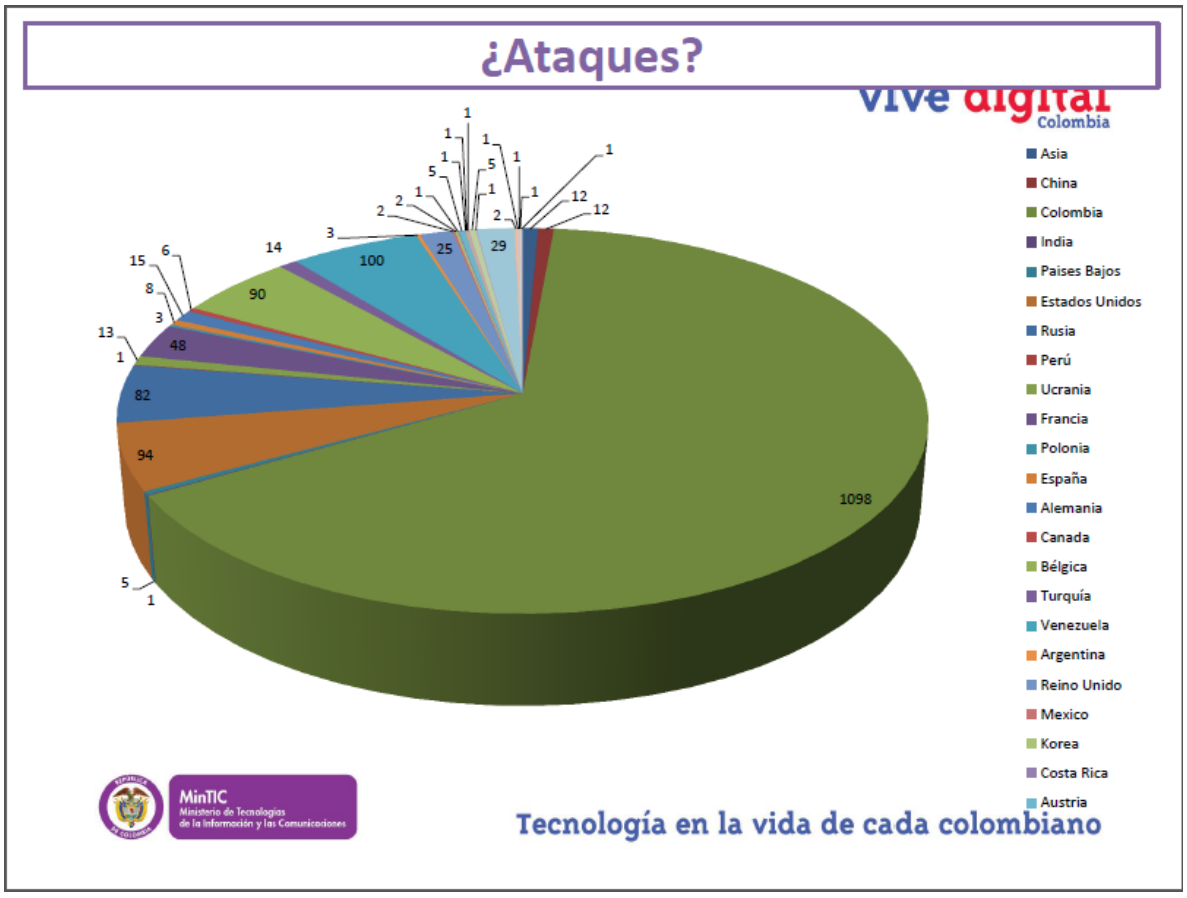
Zambrano Fabián, Tamayo Héctor (2014) Delitos Informáticos La confianza, principal herramienta para los delincuentes, Recuperado de http://www.ccit.org.co/files/SEGURIDAD%20INFORMATICA/Delitos_Informaticos.pdf

ISO (2005). Políticas de Seguridad Informática. Norma ISO / IEC 27001.

Segu-Info, (2014) Políticas de Seguridad. Recuperado de https://segu-info.com.ar/politicas/

Anónimo. Políticas de seguridad informática en una empresa, Políticas más comunes en las empresas. Recuperado de https://whxiuynnlfynnfy5/ejemplos-de-politicas-de-seguridad-informatica-en-una-organizacion/

ANEXOS


¿Ataques?
vive digital Colombia
Asia
China
Colombia
India
Paises Bajos
Estados Unidos
Rusia
Perú
Ucrania
Francia
Polonia
España
Alemania
Canada
Bélgica
Turquía
Venezuela
Argentina
Reino Unido
Mexico
Korea
Costa Rica
Austria
1098
94
82
48
90
100
29
MinTIC
Ministerio de Tecnologías de la Información y las Comunicaciones
Tecnología en la vida de cada colombiano