Delitos informáticos que pueden afectar la cadena de suministro en la norma BASC

Presentado por:

Cristhell Tatiana Londoño código 0800759

Universidad Militar Nueva Granada

Facultad de relaciones Internacionales Estrategia y Seguridad

Programa de Administración de la Seguridad y Salud Ocupacional

Bogotá D.C. 21 de Febrero 2017

Delitos informáticos que pueden afectar la cadena de suministro en la norma BASC

Resumen

El documento hace un esbozo de la denominada ciber delincuencia y los efectos dañinos que podría generar en las empresas certificadas en BASC, por ser un tema de alta importancia y realmente poco conocida, el avance de las tecnologías de la información en el entorno empresarial ha incrementado el uso de medios tecnológicos con fines delictivos en todo el mundo.

De la misma manera hace una revisión sobre el ciberdelito y las diferentes formas de ejecución del delito tomando como referencia lo tratado en los acuerdos internacionales y observa la situación en Colombia, determinando las modalidades así como los análisis que se han hecho sobre el tema, en especial en el aspecto legal.

Una vez identificada la realidad de este quebrantamiento de la ley se hace una relación de la norma BASC con respecto a la comisión de ese delito y las posibilidades reales que ocurra dentro de las empresas exportadoras con afectación a la cadena de suministro, se termina ofreciendo una recomendación sobre qué sistemas, equipos y medidas tomar frente a la realidad de una amenaza que está en crecimiento en todo el mundo

Palabras claves

Delincuencia, Amenaza informática – Ciberespacio - Ciberdefensa –

Ciberseguridad - Seguridad de la información - ciberdelito, seguridad, BASC.

Glosario

Análisis y evaluación de riesgo: Uso sistemático de la información disponible para determinar las posibles amenazas, sus causas, probabilidad de manifestación y la magnitud de sus consecuencias. (Definición tomada del glosario de términos, norma y estándares BASC)

Cadena de suministro: Es la secuencia de interacción entre los generadores de productos y servicios con sus proveedores que contribuyen en la realización, comercialización y entrega de una mercancía o un servicio a un cliente final en cualquier destino. (Definición tomada del glosario de términos, norma y estándares BASC).

Sistema de Gestión de Seguridad de la Información (SGSI): Consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización

Computadores "zombis": Denominación que se asigna a computadores personales que tras haber sido infectados por algún tipo de malware, pueden ser usadas por una tercera persona para ejecutar actividades hostiles. Este uso se produce sin la autorización o el conocimiento del usuario del equipo.

Defacement: Es una palabra inglesa que significa desfiguración y es un término usado en informática para hacer referencia a la deformación o cambio producido de manera intencionada en una página web por un atacante que haya obtenido algún tipo de acceso a ella, bien por algún error de programación de la página, por algún bug en el propio servidor o por una mala administración de este."

Keylogger: Es un software o hardware que puede interceptar y guardar las pulsaciones realizadas en el teclado de un equipo que haya sido infectado. Este malware se sitúa entre el

teclado y el sistema operativo para interceptar y registrar la información sin que el usuario lo note. Además, un keylogger almacena los datos de forma local en el ordenador infectado y, en caso de que forme parte de un ataque mayor, permite que el atacante tenga acceso remoto al equipo de la víctima y registre la información en otro equipo.

Phishing: El término proviene de la palabra inglesa "fishing" (pesca), haciendo alusión al intento de hacer que los usuarios "muerdan el anzuelo". Siendo uno de los métodos más utilizados por delincuentes cibernéticos para obtener información confidencial de forma fraudulenta. El estafador, conocido como phisher, se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico, o algún sistema de mensajería instantánea, redes sociales SMS/MMS, a raíz de un malware o incluso utilizando también llamadas telefónicas.

Smishing, Es un nuevo tipo de delito o actividad criminal a base de técnicas de ingeniería social con mensajes de texto dirigidos a los usuarios de telefonía móvil. Se trata de una variante del phishing.

Spyware: Es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

Vishing: Es una variante del Phishing, consiste en enviar correo electrónico en el cual los delincuentes consiguen datos bancarios mediante los números telefónicos gratuitos de las entidades bancarias, simulan la computadora y piden los datos de cuentas, claves, PIN.

Introducción

La aparición de nuevas tecnologías además de generar conocimientos y destrezas, también abrió la puerta a la delincuencia, en el caso de los desarrollos ciber, trajo consigo la delincuencia especializada en este campo, que no es otra cosa que la disposición a vulnerar los sistemas de seguridad apalancados en las herramientas ciber de diversas organizaciones.

Las empresas involucradas en el proceso del comercio internacional han sido o podrían ser afectadas por este tipo de ilícito de manera directa o indirecta, en especial en la denominada cadena de suministros; el autor propone desarrollar un proceso de identificación de los delitos informáticos que amenazan la cadena de suministro con relación a los estándares aplicados por la norma BASC, con el fin de contextualizar la constante evolución en el área de la tecnología informática, y prevenir los posibles ataques informáticos que atenten contra los activos de las organizaciones.

Para lo anterior es primordial ante todo hacer una breve descripción de cada una de estas acciones delictivas que afectan los sistemas informativos, y partiendo de ello prevenir los efectos negativos que puedan generar en la cadena de suministros de una organización.

Posterior a ello es adecuado hacer un análisis de los estándares BASC con respecto a la efectiva implementación de un SGCS, enfocado a la prevención del delito ciber y finalmente proponer alternativas que permitan hacer una adecuada gestión de los riesgos de la ciber delincuencia para proteger los activos de una organización.

Interesarse en el tema de la ciber delincuencia y lo que afectaría las empresas certificadas en BASC, es una preocupación nacida de la experiencia vivida en la formación como auditor, basado en que la norma es de alta importancia en el sector del comercio internacional y el tema

propuesto puede tomarse como elemento complementario al momento de efectuar una certificación, de la misma manera es una inquietud por adentrarse en un tema de seguridad poco estudiado y de amplias repercusiones en la seguridad actual.

Tenido como antecedente el concepto de Seguridad informática de Ramio "Un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas. Concienciarlas de su importancia en el proceso será algo crítico" (2006. Pág. 50), es para el autor importante tomar el tema de ciberseguridad como un propósito de estudio bajo el precepto que es pertinente para un profesional de seguridad conocer de ello.

La seguridad es fundamental en toda empresa, ahora bien, qué tan preparado está el especialista en seguridad para afrontar el reto de involucrarse a proteger una empresa en donde su desarrollo se basa en los datos que fluyen por la red?, la respuesta podría ser incierta; Por ello la ciberseguridad debe ser una prioridad, el director de seguridad debe prepararse y ser protagonista en protección de datos y contribuir en generar herramientas para su resguardo, sin ocasionar trabas en el funcionamiento de la empresa, la solución no es desconectarse, es tener el sistema seguro, se tendrán que aplicar políticas, metodologías y técnicas de protección de la información porque la conectividad es vital.

Los delitos informáticos

Con frecuencia en los últimos años se conoce la ocurrencia de los denominados delitos informáticos que afectan cualquier empresa, muy pocas veces hay claridad sobre cómo es que se cometen, se podría decir que eso es tema de especialistas, ingenieros forenses, expertos internautas o los denominados hacker blancos que trabajan en pro de la seguridad informática.

Entonces qué es el delito informático? tomando como referencia el Convenio de Ciberdelincuencia del Consejo de Europa [i], se puede definir como: "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos", es una definición que claramente indica tres aspectos fundamentales la confidencialidad, integridad y disponibilidad, aspectos básicos de toda información independiente de donde este consignada.

Una de las razones que esgrime BASC tiene relación con "la preservación, custodia y confidencialidad", si esto se lleva al tema de la Ciberdelincuencia es evidente que hay que establecer mecanismos muy precisos para evitar la ocurrencia de incidentes de esta naturaleza que podrían afectar el normal cumplimiento de las actividades empresariales.

Es pertinente aclarar que actualmente, el Convenio sobre la Ciberdelincuencia del Consejo de Europa es el único acuerdo internacional que cubre todas las áreas relevantes de la legislación sobre ciber delincuencia (derecho penal, derecho procesal y cooperación internacional). Adoptado por el Comité de Ministros del Consejo de Europa en su sesión N. 109 del 8 de noviembre de 2001, se presentó a firma en Budapest, el 23 de noviembre de 2001 y entró en vigor el1 de julio de 2004.

El Convenio de Budapest, que entró en vigor hace 15 años, ha sido ratificado por 41 de los 47 Estados miembros del Consejo de Europa y por 4 del continente americano (Estados Unidos, Canadá, Panamá y República Dominicana) según estadísticas que presenta el Concilio de Europa en su sitio web de seguimiento al Convenio, países como Perú, Colombia, Paraguay o Argentina ya han reformado su legislación de acuerdo con el Convenio de Budapest.[ii] En 2013, a través del Ministerio de Relaciones Exteriores, Colombia solicitó formalmente la adhesión a esta convención.

La OCDE emitió, el 17 de septiembre de 2015, las recomendaciones sobre gestión de riesgos de seguridad digital para la prosperidad económica y social, dicho documento da consejos sobre estrategias y políticas de seguridad digital que los países deben tener bajo un modelo institucional eficiente y de vinculación integral de las múltiples partes interesadas.

Puede afirmarse del delito informático que es difícil de demostrar en atención a que las pruebas sobre su ocurrencia presentan dificultad de consolidarse, es ejecutado de manera remota, basta tener acceso a la red, un equipo adecuado y los conocimientos necesarios, además que implica escasos segundos para ejecutarse, en el momento actual de los negocios en donde todo está interconectado y que, según las autoridades ha evolucionado y su tendencia es al crecimiento.

Las modalidades que involucra el delito informático son conocidas como el empleo de medios electrónicos para vulnerar sistemas de información, con el objetivo de acceder a servicios de un usuario determinado que esté empleando la tecnología para obtener información confidencial, en este caso empresarial para obtener beneficios de cualquier índole, especialmente económicos.

El anexo "A", contempla la Legislación 1273 Delitos Informáticos en Colombia ésta se promulgó en el 2009, en donde se crean nuevos tipos penales relacionados con la afectación a los sistemas informáticos y la protección de la información y de los datos sobresalen los siguientes:

• Artículo 269A: Acceso abusivo a un sistema informático.

• Artículo 269B: Obstaculización ilegitima de sistema informático.

• Artículo 269C: Interceptación de datos informáticos.

• Artículo 269D: Daño Informático.

• Artículo 269E: Uso de software malicioso.

• Artículo 269F: Violación de datos personales.

• Artículo 269G: Suplantación de sitios web para capturar datos personales.

• Artículo 269H: Circunstancias de agravación punitiva.

• Artículo 269I: Hurto por medios informáticos y semejantes.

• Artículo 269J: Transferencia no consentida de activos.

Otras leyes que también tienen que ver con el tema de seguridad y protección de datos, La ley 1581 establece un marco para la protección de datos, divulgación y denuncia de las violaciones de seguridad; circular de la superintendencia financiera 052 de 2007, que trata de los estándares de seguridad y calidad para el manejo de la información a través de medios y canales de distribución de productos y servicios; decreto 1704 de 2012 que trata de interceptación legal de comunicaciones; decreto ley 019 de 2012, que trata sobre las entidades de certificación digital

Esta legislación es amplia, se considera suficiente, involucra todos los aspectos pero existe una dificultad, en palabras de Andrés Guzmán, CEO de la firma Adalid Corp, especializada en investigaciones de este tipo "La legislación colombiana de delitos informáticos es suficiente, el problema es de conocimiento en la materia de parte de jueces, fiscales y organismos de policía judicial"... “no existen fiscales ni jueces especializados en delitos informáticos”; así que este es el panorama al que se enfrenta las empresas colombianas frente a este tipo de ilícito, los especialistas afirman que la justicia no está preparada para enfrentar este delito, aspecto que puede ser cierto o no, por ello la empresa debe fortalecer sus sistemas de seguridad.

El gobierno Colombiano sigue en su actuación, al respecto el documento 3701 CONPES (Consejo Nacional de Política Económica y social), hace precisiones sobre lineamientos de política para ciberseguridad y ciberdefensa, en uno de sus apartes iniciales indica:

> “El aumento de la capacidad delincuencial en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común a todos los

países, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado e incluyendo a la sociedad civil". (2011, pág. 4)

Se nota que el Estado colombiano se ha preocupado y se prepara para afrontar este accionar delictivo que afecta el sector público y privado, generando dinámicas de concertación, legislación, y acogiéndose a acuerdos internacionales en beneficio de la comunidad nacional e internacional que se relaciona con el país.

En concordancia con el anterior aparece en 2016 el CONPES 3854, que trata sobre la política nacional de seguridad digital, es decir amplía el espacio de conocimiento sobre lo digital, en búsqueda de ofrecer una política pública amplia y suficiente que brinde plenas garantías de seguridad en el tema digital. Lo característico es que hace el estudio tomando en consideración 5 ejes estratégicos

1. Establecer un marco institucional en torno a la seguridad digital
2. Crear condiciones para que las partes interesadas gestionen los riesgos de seguridad.
3. Fortalecimiento de la defensa y seguridad digital a nivel nacional e internacional
4. Adecuación de un marco regulatorio para comportamientos responsables en entornos digitales.
5. Mecanismos permanentes de cooperación, colaboración y asistencia en seguridad digital a nivel nacional e internacional.

Las operaciones de las empresas cada día están más relacionadas con el manejo de canales de internet y telefonía móvil; al respecto la Superintendencia Financiera indica que en Colombia en el primer semestre de 2016 "El sistema financiero reportó 1.119.286.723 operaciones realizadas en el canal Internet; 166.679.939 monetarias por $1.193,2 billones de pesos y 952.606.784 no monetarias" de la misma forma a través del canal de telefonía móvil "reporto 84.547.821

operaciones realizadas en el canal Telefonía Móvil; 14.164.207 operaciones monetarias por $2,3 billones de pesos y 70.383.614 no monetarias"[iii].

Las cifras son claras, se mueven billones de pesos a través de canales que fácilmente podrían ser afectados por el ciberdelito, por ello las empresas en especial del sector exportador o que tienen transacciones a nivel internacional han de tomar medidas urgentes y bien planteadas que permitan afrontar este riesgo elevado.

Con respecto al dicho ilícito, el observatorio de ciberseguridad de la Policía Nacional indica que en el lapso de enero de 2015 a enero de 2017 se han presentado incidentes de seguridad informática de acuerdo a la siguiente tabla.

Tabla 1: Incidentes de ciberseguridad denunciados

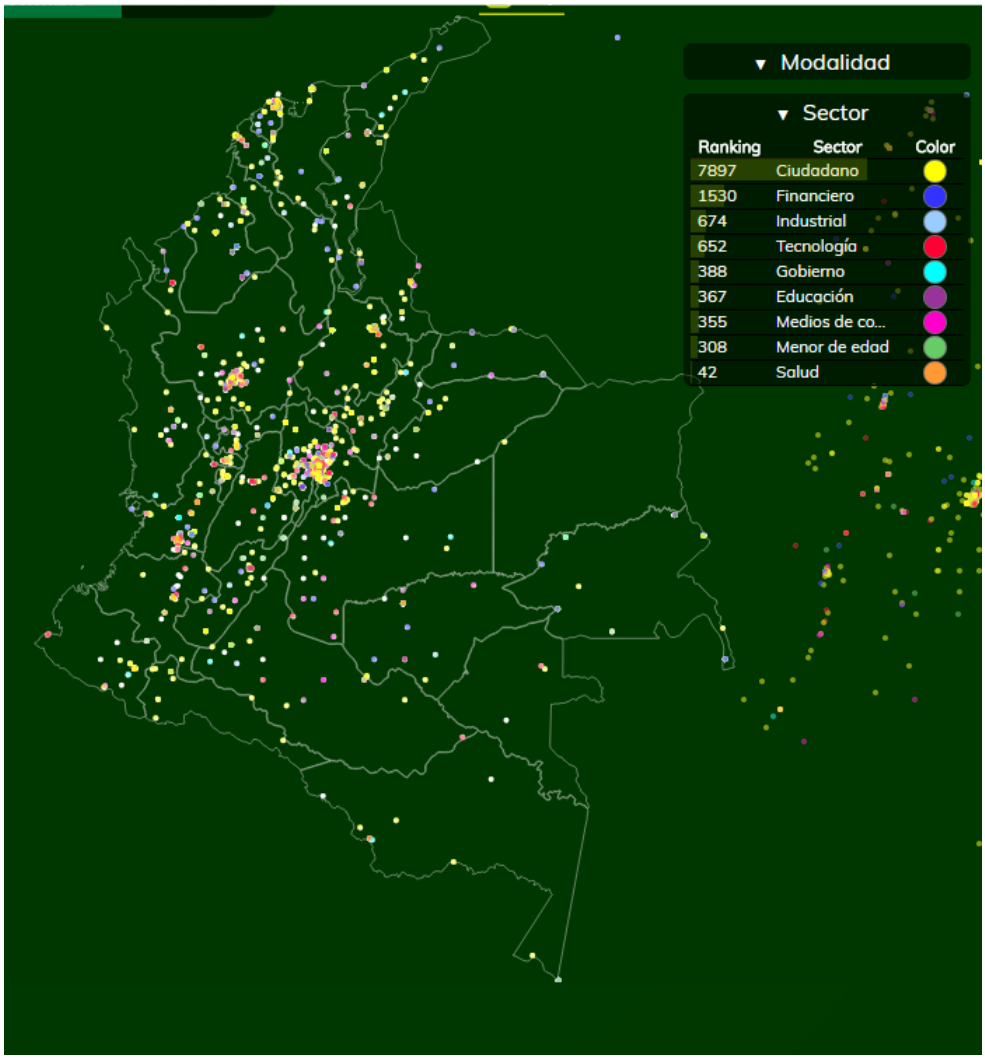
Modalidad		Sector		Delito	
Ranking	Modalidad	Ranking	Sector	Ranking	Delito
1838	Estafa por compras	7737	Ciudadanos	2860	Articulo 246 Estafa
1278	Suplantación de identidad	1513	Financiero	972	No especificado
1024	Phishing	388	Gobierno	1331	Articulo 239 Hurto
568	Smishing *	673	Industrial	1459	Articulo 269 A
715	Atraco	620	Tecnología	924	Articulo 269 F
481	Injuria / calumnia	366	Educación	929	Articulo 269 G
642	Vishing *	344	Medios de comunicación	650	Articulo 347
931	Defacement *	301	Menor de edad	191	Articulo 220 injuria
495	Amenazas	42	Salud	504	Articulo 269 E
462	Malware			405	Articulo 269 I

Fuente: Elaborado con base a información obtenida del observatorio de ciberseguridad policía nacional, http://www.ccp.gov.co/ciberincidentes/tiempo-real/historico, en línea, consultado el 05 de enero de 2017

Las cifras muestran una realidad que aqueja en general a todo el conglomerado social, todos los sectores y se presenta en todo el país, lo cual se evidencia en el siguiente mapa, que muestra en tiempo real, graficado en colores el sector afectado por el cibercrimen, de acuerdo a

denuncias formuladas, de este mapa se puede concluir que la mayor parte de incidentes se dan en las zonas de mayor desarrollo industrial, comercial y en los conglomerados urbanos.

Imagen 1: Mapa de sectores afectados por cibercrimen de acuerdo a denuncias



Fuente: Información obtenida del observatorio de ciberseguridad policía nacional, http://www.ccp.gov.co/ciberincidentes/tiempo-real/historico, en línea, consultado el 05 de enero de 2017

Se hace la aclaración que esta estadística es elaborada con base a denuncias y en el contexto colombiano no hay una costumbre marcada de informar a las autoridades cuando se es víctima

de la ocurrencia de cualquier ilícito, así que la magnitud de la transgresión es mucho más allá de lo evidenciado.

El tema es de preocupación internacional, el fundador de la Compañía de computo forense Mattica en México, Andrés Velásquez, refiriéndose a la judicialización de este delito indicó citado por Pérez "El reto más grande es que a pesar de que existe la Ley pocos jueces la entienden y a veces los fiscales no logran documentar los casos e identificar si realmente las conductas entran dentro de la tipificación de los delitos o no",(2013) es decir aún hay falencias en el sistema jurídico para judicializar y sancionar de manera acertada a quienes los cometen.

Así que la intranquilidad de toda empresa es estar a la vanguardia frente a la posibilidad de ser víctima del ataque informático, al respecto en palabras de Paul Proctor, vicepresidente y analista de Gardner.[iv] "Las organizaciones deberán aprender a vivir con niveles aceptables de riesgo digital así como a la unidades de negocio deben descubrir qué seguridad necesitan y qué pueden permitirse. La ética digital, el análisis y un enfoque centrado en las personas pueden ser más importante que los controles técnicos", esta aseveración se torna valiosa puesto que el autor hace énfasis en el control de las personas por encima de cualquier aditamento tecnológico de última generación, es lógico, las personas son quienes fallan y hace mal uso del sistema

Información obtenida en un estudio efectuado en Estados Unidos en 2016, por Disterman Research e Intel Security [v], la mayoría de ataques se presentaron en el sector salud y financiero, el ingreso a las organizaciones se dio a través de correo electrónico 30%, archivo adjunto a email 28%, Sitio web diferente a redes sociales 24%; redes sociales 4%; memorias USB3%; aplicación de negocios 1%; no se sabe 9%. El mismo estudio indica que la afectación en las empresas se dio de la siguiente manera: Se tuvo que parar la operación 12%; afectación directa a las personas

78%; empleo de equipos propios por afectación de los corporativos 11%; pérdidas monetarias 6%.

En el artículo “predicciones en seguridad para 2017” de la revista digital Nro. 10, diciembre de 2016, CSO, España, reitera que los empleados son el eslabón más débil de la seguridad y por lo general casi todos los ataques empiezan con Phishing, aunque todos los empleados estén entrenados en buenas prácticas de seguridad, porque siempre el ser humano será falible; estadísticas mencionadas por Melchor Sanz, director de preventa de HP. Indican que el 66% de los riesgos de una empresa están iniciados por un mal hábito del usuario.

Determinar el daño o afectación a los servicios informáticos que podrían afectar una compañía certificada en BASC, no puede ser un caso particular, tal vez se puede afirmar que esta amenaza afecta todas las empresas, la ventaja que tienen las que estén certificadas en BASC es que tal vez podrían estar o deberían estar mejor preparados para afrontarlos dado que el sistema de certificación contribuye positivamente en este campo, por ello una de las recomendaciones de BASC es que se “disponga de un sistema de protección y recuperación de la información sensible de la organización que incluya medios magnéticos y físicos”.

El “convenio sobre Ciberdelincuencia, del 1 de noviembre de 2001, hace una clasificación de la siguiente manera:

1. Delitos contra la confidencialidad, la integridad, y la disponibilidad de los datos y sistemas informáticos.

Art. 2: Acceso ilícito

Art. 3: Interceptación ilícita

Art. 4: Interferencia en los datos (Ataques a la integridad de los datos)

Art. 5: Interferencia en el sistema (Ataques a la integridad del sistema)

Art. 6: Abuso de los dispositivos

2. Delitos informáticos.

Art. 7: Falsificación informática

Art. 8: Fraude informático

3. Delitos relacionados con el contenido.

Art. 9: Delitos informáticos relacionados con la pornografía infantil

4. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.

Art. 10: Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Con respecto a las modalidades y acciones complementarias que llevan inmerso este ilícito se pueden denominar de la siguiente manera, haciendo la aclaración que en todos los países no se denominan igual, para el presente documento se toman referencias de las acepciones gramaticales propias de Colombia:

- Falsificación de documentos vía computarizada (tarjetas de crédito, cheques)
- Variación de los activos y pasivos en la situación contable de las empresas.
- Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude)
- Lectura, sustracción o copiado de información confidencial.
- Modificación de datos tanto en la entrada como en la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
- Uso no autorizado de programas de cómputo.

- Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.
- Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
- Obtención de información residual impresa en papel luego de la ejecución de trabajos.
- Acceso a áreas informatizadas en forma no autorizada, a través de computadores “zombis”
- Intervención en las líneas de comunicación de datos o teleproceso.
- Programación de instrucciones que producen un bloqueo total al sistema.
- Destrucción de programas por cualquier método.
- Daño a la memoria.
- Atentado físico contra la máquina o sus accesorios.
- Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
- Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).
- TERRORISMO
- Sabotaje
- Narcotráfico
- Espionaje, espionaje industrial
- el tráfico de armas,
- proselitismo de sectas,
- propaganda de grupos extremistas,

Vistas las consideraciones anteriores se precisa mencionar que la ciberseguridad debe ser parte esencial de toda empresa en especial de aquellas involucradas en el contexto internacional, una falla en el sistema o un ataque podría hacer que la mercancía llegue a otro puerto de destino, sea desechada o incluso contaminada a través de procedimientos articulados por un malware (programa maligno)

BASC, la norma y su relación con el delito informático

Lo descrito hasta ahora muestra una realidad que afecta la seguridad de las empresas, haciendo revisión de la norma BASC se puede hacer las siguientes apreciaciones:

Es evidente, todos los ataques malintencionados al sistema informático pueden afectar la "cadena de suministro" de la entidad, por consiguiente se prestara atención a los diferentes procesos que hacen uso de las redes de comunicación; ¿En dónde entonces se aplicarían las medidas de seguridad que protejan la compañía?, es la preocupación del empresario.

Para encontrar la respuesta de acuerdo con la norma, la organización debe crear un adecuado "sistema de gestión en control y seguridad SGCS", del cual se indica que es una "Estructura de seguridad con enfoque de procesos basada en la gestión de riesgos de la cadena de suministros y soportada en la mejora continua, que ayuda a lograr los objetivos de la organización, mediante la implementación de los requisitos de esta Norma y de los Estándares BASC.

En general la afectación de la seguridad pasa por alterar algún tipo de documento, al respecto la norma BASC lo refiere como "Información y su medio de soporte o registro, especificación, procedimiento documentado, plano, informe, norma. El medio de soporte puede ser papel, disco magnético, óptico o electrónico, fotografía o muestra patrón o una combinación de éstos", tomando como reseña ésta aseveración, la documentación manejada a través de sistemas

informáticos relacionada con procesos de almacenamiento, embalaje, despacho y transporte de las mercancías debe ser protegida contra cualquier manipulación o introducción de datos erróneos y por ello, no debe tener espacios en blanco, así mismo los equipos con los cuales se tramitan y mantiene la documentación deben ser seguros, protegiéndola de cualquier daño o pérdida.

Entonces ¿de dónde provendrá el ataque que afecte el sistema informático o a través de qué dispositivo de la empresa se originará el ataque?, pues bien, el ataque procede a través de la red, y se entiende que pueden ser mediante el uso fraudulento de cada uno de los equipos de cómputo conectados a la red de la empresa, los dispositivos móviles con acceso a wifi, las impresoras, en fin todo equipo con posibilidades de acceso a información de manera física o remota.

De manera complementaria aunque la norma no lo indica se enuncian algunas medidas de seguridad, las cuales nacen desde el mismo entorno físico de ubicación del sistema; por un lado se debe proteger el Hardware (conexión del servicio eléctrico, seguridad contra incendios, accesos biométricos, sistema de extinción de incendios de gas, climatización y enfriamiento) y por consiguiente el Sofware (firewalls, anti-malware, sistemas de detección y prevención de intrusos, sistemas de gestión y correlación de eventos para análisis en tiempo real, redundancia de conectividad), pero por encima de todo ello, está la prevención y un equipo humano altamente calificado en seguridad.

Cualquier estándar de seguridad en la cadena de suministro se complementará necesariamente con un adecuado análisis de riesgo, no basta con proponer medidas de seguridad comunes, el riesgo es particular, único e irrepetible en cada corporación, por ello es que en las empresas asociadas a BASC se requiere de un alto compromiso de la dirección en la empresa en el tema de seguridad de la cadena de suministro.

De la misma forma debe adelantarse una permanente "auditoria del sistema de control y seguridad SGCS", definida por BASC como "Examen sistemático, objetivo e independiente, para determinar si las actividades y resultados relacionados con la gestión en control y seguridad, cumplen las disposiciones preestablecidas y si estas se aplican en forma efectiva y son aptas para alcanzar los objetivos", la cual llevara a identificar con certeza hasta donde el sistema está asegurado.

De la misma forma hace BASC referencia a las políticas y de ellas de manera acertada indica que referirse a ellas significa que:

> La primera manifestación en contra de que la compañía sea utilizada por organizaciones ilícitas, es de sus dueños, directivos o administradores; estas son de carácter general y sirven como base para que cada área de la compañía, escriba sus propias políticas.

Esto indica precisamente que es la empresa y nadie más la responsable de establecer sus mecanismos de control de acuerdo a su labor, función, negocio puesto que del interior de la organización es que se sabe el riesgo que se corre.

Algunas medidas de seguridad generales que las empresas deberían instaurar

El anexo "B", contiene una política de seguridad completa, no obstante se enuncian algunas medidas que de ser aplicadas en las organizaciones contribuyen al mejoramiento de la seguridad informática.

- Todas las dependencias donde existan equipos de comunicación deben tener control de acceso además en el área del servidor principal no se permitirá la entrada a personal no autorizado.
- Todos los equipos de la compañía deben protegerse por software de detección y reparación de virus.
- Sistemas de prevención contra intrusos (Firewall)

- Instalar sistemas detectores de vulnerabilidades (Netclarity) que previene frente acciones forzosas o no autorizadas.
- En la entrada de la empresa se lleva registro de ingreso para el control de elementos ajenos a la entidad controlada por el vigilante.
- Instalar un sistema anti spam al servicio de correo electrónico para controlar el ingreso de correos no deseados y propagación de virus
- La información contenida en memorias USB debe ser encriptado con un aplicativo que se llama Bitlocke para evitar la fuga de información.

En el tema de la ciberseguridad debe asegurarse absolutamente toda la cadena, no solo un eslabón, porque el riesgo mutaría a otros eslabones no protegidos, especialmente teniendo en cuenta que la información confiable es la base para la toma de decisiones acertadas y si esta información ha sido cuidadosamente protegida no se presentan alteraciones o afectaciones en el cumplimiento de procesos exportadores.

Por consiguiente hay que cumplir al pie de la letra los estándares del SGCS, los cuales aparte de ser de obligatorio cumplimento sirven como herramienta complementaria para detectar, evidenciar y contrarrestar cualquier intento de ataque, los cuales además de ser útiles son adecuados para los objetivos de seguridad pretendidos por la empresa que está asociada a BASC.

Recomendaciones

La organización ha de tomar conciencia de la importancia de la tecnología al interior de los procesos y actividades de comercio internacional por ello es indispensable que adopte controles extremos en el manejo de la información magnética, de la misma forma controles para el manejo de los sistemas informáticos, asignando claves de acceso a cada usuario, efectuar copias de respaldo de la información que se maneja a diario, formación permanente en seguridad

informática, medidas de prevención, emitir criterios o normas de manejo documental cuyo conocimiento sea sólo para un determinado nivel de autoridad en la empresa, clasificarlos bajo rótulos de reservado, restringido o confidencial y medidas de alerta temprana frente a cualquier señal de amenaza.

Contar con un lugar apropiado para el archivo de los documentos digitales y la información, es prioritario sin afectar la disponibilidad e integridad de la misma, en la actualidad se manejan las denominadas nubes en donde el usuario con todas las medidas de seguridad puede albergar su información con mínimos riesgos.

También y muy relacionado con BASC, se puede tomar como referencia lo que indica la norma ISO 27000 [vi] respecto a que la empresa debe hacer procesos de "Adquisición, desarrollo y mantenimiento de sistemas de información: Asegurar la inclusión de todos los controles de seguridad en los sistemas de información nuevos o en funcionamiento (infraestructura, aplicaciones, servicios, etc.). También regula la adquisición de software para la organización y los contratos de soporte y mantenimiento asociados a ellos", es decir hay que invertir en seguridad en todos los sistemas de información de la empresa.

Durante el proceso de investigación se conocieron sistemas y dispositivos de última generación los cuales podrían ser empleados o instalados por las empresas certificadas en BASC para protegerse del ciber ataque o ciber delito. Brevemente se detallan algunos sistemas, tomados del artículo "La ciberseguridad, centro de atención de las organizaciones en la era digital", de la revista digital Nro. 10, diciembre de 2016, CSO, España.

1. La compañía ha incorporado un **sistema de chip criptográfico TPM** (Módulo de Plataforma Segura) en sus impresoras que aloja las credenciales de acceso de los usuarios y ha desarrollado la solución **HP Sure Start**, tecnología que permite la detección y autorreparación de ataques maliciosos a la BIOS (Sistema Básico de Entrada y Salida). Estas funciones han conseguido que las nuevas impresoras láser de HP sean consideradas las más seguras del mundo.

2. Panda Security ha desarrollado **Adaptative Defense 360**, una solución que nace en la nube de Panda y monitoriza constantemente el *Endpoint*: detecta proactivamente los ataques, recopila la información necesaria para responder a las violaciones de seguridad y aplica acciones de remediación de forma automática para minimizar el impacto y el alcance de la infección.
3. **La plataforma inteligente de Akamai** proporciona servicios de entrega de contenido y servicios de seguridad, tanto para ataques lanzados contra el entorno web como para proteger los activos de sus clientes. El software de la compañía genera mapas de internet de forma continuada para obtener información detallada de las condiciones de la red, detectar instantáneamente dispositivos e identificar, absorber y bloquear las amenazas.

Las empresas deben vincularse y acudir a centros de apoyo especializados como el CSIRT-CCIT, Centro de coordinación seguridad informática Colombia, la cual según su portal es:

> Un centro de coordinación de atención a incidentes de seguridad informática Colombiano, el cual está en contacto directo con los centros de seguridad de sus empresas afiliadas y está en capacidad de coordinar el tratamiento y solución de las solicitudes y denuncias sobre problemas de seguridad informática que sean recibidas en la cuenta de correo electrónico contacto ATcsirt-ccit.org.co Actualmente se están efectuando trabajos en contra del robo de información privada (phishing), la cual es usada posteriormente para sustraer dinero de las cuentas bancarias de las víctimas. Estas tareas anti-phishing se están realizando, de forma coordinada, entre las entidades bancarias y las empresas prestadoras del servicio de Internet que están agrupadas en el NAP Colombia.

Esta entidad podría convertirse en un aliado de negocio puesto que provee asistencia y apoyo frente a la ocurrencia de cualquier tipo de afectación al sistema informático de la empresa

Respecto a la formación académica, lamentablemente el sistema educativo colombiano, no hace énfasis en esta materia, tal como lo indica el CONPES 3701

> El conocimiento en el área de ciberseguridad y ciberdefensa tanto en el sector público como en el privado es limitado. Si bien en el país existen algunas instituciones de educación superior que ofrecen especializaciones en seguridad informática y derecho informático, se ha identificado que la oferta académica en programas especializados en estas áreas es reducida. En consecuencia, un

> número significativo de personas que acceden a algún tipo de formación en el área de seguridad de la información, lo hacen mediante programas ofrecidos por instituciones extranjeras, en los que no se profundiza sobre la realidad colombiana. (2011, pág. 18)

Este documento es claro, la formación que se ofrece en temas de seguridad tanto a nivel técnico como tecnológico y universitario no contiene la suficiente profundización, tal como lo indica acertadamente el referido escrito público.

El autor considera que el profesional de Administración de Seguridad necesariamente debe adquirir habilidades en todos los temas relacionados con la Seguridad Informática, la cual es necesaria en la empresa para la protección, mantenimiento, control de acceso, confidencialidad, integridad y disponibilidad de la información, tanto para la seguridad de la información como para la seguridad en el soporte de las operaciones de las organizaciones,

En concepto del autor, los nuevos delitos nacidos de la evolución de los sistemas informáticos y que se denominan entre otros cibercrimen, ciberataque, y ciberseguridad, deben constituirse en tema de profundo estudio para mantenerse a la vanguardia en todo lo relacionado con los delitos de actualidad.

Bibliografía

Centro de Información y Respuesta Técnica a Incidentes de Seguridad Informática de Colombia Cirtisi – Colombia

Consejo Nacional de política Económico y Social (CONPES) 3701.Departamento Nacional de Planeación. Lineamientos de política para ciberseguridad y ciberdefensa. Julio de 2011

Consejo Nacional de política Económico y Social (CONPES) 3854.Departamento Nacional de Planeación. Política nacional de seguridad digital. Abril de 2016

Guía de seguridad para los actores de la cadena de suministro. 2013**.** *"Herramienta práctica para la prevención de riesgos asociados a la seguridad"* Policía Nacional Dirección de Investigación Criminal e INTERPOL Frente de Seguridad Empresarial *Cuarta edición. Bogotá. Rasgo y Color SAS.*

Ministerio De Defensa, Policía Nacional, Observatorio de ciberseguridad, centro cibernético policial http://www.ccp.gov.co/ciberincidentes/tiempo-real/historico, en línea, consultado el 05 de enero de 2017

Ramio A. Jorge. 2006. Libro Electrónico de Seguridad Informática y Criptografía, Universidad Politécnica de Madrid, España - copyright 2006.

ISO/IEC 27001 estándar para la seguridad de la información, se encuentra normalizada por el Instituto Colombiano de Normas y Técnicas y Certificación ICONTEC.

World BASC Organization Business Alliance for Secure Commerce (BASC) GLOSARIO DE TÉRMINOS Norma y Estándares BASC. Versión: 04-2012. Aprobado: Julio 16 de 2012.

https://es.wikipedia.org/wiki/Defacement, en línea, consultado el 05 de enero de 2017

https://es.wikipedia.org/wiki/Smishing, en línea, consultado el 05 de enero de 2017

http://www.cibanco.com/work/models/cibanco/Resource/2011/1/images/Vishing.pdf, en línea, consultado el 05 de enero de 2017.

http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf. En línea, consultado el 05 de enero de 2017

http://www.todoiure.com.ar/monografias/mono/ penal/Definiciones_de_delito.htm.

http://cso.computerworld.es/seguridad-en-cifras/el-60-de-las-empresas-sufrira-grandes-fallos-en-sus-servicios-en-2020. En línea, consultado el 05 de enero de 2017

https://colombiadigital.net/actualidad/articulos-informativos/item/4810-en-colombia-se-investigan-los-delitos-informaticos.html.Articulo escrito por Camilo Pérez García En línea, consultado el 05 de enero de 2017

https://www.superfinanciera.gov.co/jsp/loader.jsf?lServicio=Publicaciones&lTipo=publicaciones&lFuncion=loadContenidoPublicacion&id=61066, en línea, consultado el 05 de enero de 2017.

[i] Adoptado por el Comité de Ministros del Consejo de Europa en su sesión N° 109 del 8 de noviembre de 2001, se presentó a firma en Budapest, el 23 de noviembre de 2001 y entro en vigor el 1 de julio de 2004.

[ii] Council of Europe, (2014).Convention on Cybercrim CETS No.: 185.Recuperado de http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.

[iii] Superintendencia financiera de Colombia, Informe de Operaciones, primer semestre de 2016, delegatura para riesgos operativos riesgooperativo@superfinanciera.gov.co, septiembre de 2016.

[iv] http://cso.computerworld.es/seguridad-en-cifras/el-60-de-las-empresas-sufrira-grandes-fallos-en-sus-servicios-en-2020

[v]Edgar Medina, Periódico el Tiempo. No. 37286. Artículo “las nuevas y aterradoras formas del cibercrimen” 15 de enero de 2015.

[vi] ISO/IEC 27001 estándar para la seguridad de la información, se encuentra normalizada por el Instituto Colombiano de Normas y Técnicas y Certificación ICONTEC.

Anexo “A”.

Legislación Delitos Informáticos en Colombia

(Por la extensión de la legislación se toman los Artículos referentes a los Delitos Informáticos, se proporciona la URL para descargar los documentos completos).

Ley 1273 del 05 de enero de 2009: "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado ―de la protección de la información y de los datos‖- y se preservan integralmente los sistemas que utilice las tecnologías de la información y las comunicaciones, entre otras disposiciones".

CAPITULO. I

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena 62 de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión

de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o

suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Artículo 58. Circunstancias de mayor punibilidad. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera:

17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos

Descargar Documento completo en:

http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Anexo "B"

Política General de seguridad informática.

Tomando como referencia las recomendaciones BASC y todo su componente las empresas certificadas en BASC han de establecer la presente política, alineada al cumplimiento de la norma con el fin de, proteger, y preservar la integridad, confiabilidad y disponibilidad de la información física y digital, a través de la implementación de controles de seguridad, con el

objetivo de garantizar el aseguramiento de la información de los procesos propios de la entidad para que sea consultada, modificada únicamente por personas autorizadas de la empresa.

Políticas de organización de seguridad de la información

Objetivo: Definir la seguridad de la información dentro de la organización.

Normas que rigen para la estructura organizacional de Seguridad de la información.

Normas Dirigidas a: funcionarios y directivos.

- Se debe promover a través de capacitaciones adecuadas el conocimiento de las políticas de Seguridad de la Información a todos los funcionarios de la empresa.
- Debe observar el cumplimiento de las disposiciones y normas relativas a proteger la propiedad intelectual.
- Se debe establecer las responsabilidad de cada funcionario frente a actividades que cada quien ejecuta preservando la confidencialidad de la información.
- Los funcionarios deben ser entrenados y enseñárseles a clasificar la información de acuerdo al uso.
- Los empleados con acceso a sistemas informáticos deben tener su cuenta individual y correspondiente contraseña, la cual debe ser cambiada periódicamente.

Normas dirigidas a: oficina de sistemas y tecnología.

- Se debe reportar, analizar y hacer seguimiento a los incidentes de seguridad que se presenten para que sean tratados del acuerdo al riesgo identificado.
- deben ser instalados y mantenidos Software Anti Virus y anti Espia entre otros en los sistemas de computación susceptible a la infiltración.
- La oficina de sistemas debe verificar el cumplimiento de las políticas de seguridad de la información de la empresa.

- La oficina de sistemas debe asignar responsabilidades a cada uno de sus funcionarios para la utilización de los recursos informáticos.
- Debe establecer políticas, procedimientos y normas de tecnología de información utilizadas en la organización, las cuales deben darse a conocer mediante capacitación.

Política de responsabilidad sobre los activos de información.

Objetivo: Asegurar que se aplica un nivel alto de protección a los activos de información de la empresa.

Normas dirigidas a: oficina de sistemas y tecnología.

- Realizar y mantener la configuración a los recursos informáticos de la empresa, para que e pueda hacer correcto uso de los mismos.
- Debería disponer de copias de respaldo de la información sensible de la organización.
- Mantener un sistema de cifrado de información en medio magnético, protegiendo la información contra divulgación, daño y/o modificaciones no autorizadas.
- Realizar inventario de equipos y aplicaciones, delegando responsabilidades a los usuarios.
- Realizar Backup de la información que manejaba un empleado cuando es retirado de la ocupación.
- Se debe indicar a los empleados que acceden al sistema informático las condiciones de uso de los recursos manteniendo su disponibilidad e integridad así como la responsabilidad inherente al cargo.
- Deben establecer un sistema para identificar el abuso de los sistemas informáticos a fin de detectar accesos no autorizados, manipulación indebida o la alteración de los datos del negocio.

Normas dirigidas a: Empleados y Directivos.

- Deben generar y mantener un inventario de los activos de información que están bajo su responsabilidad.
- En los contratos se deben establecer acuerdos de confidencialidad, para prevenir que la información sea divulgada a terceras personas no autorizadas.
- La información debe mantenerse asegurada de acuerdo a la clasificación establecida por la empresa.

Política de seguridad dirigida al recurso humano.

Objetivo: Asegurar que los funcionarios cumplan sus responsabilidades y obligaciones respecto a la política de seguridad, para reducir el riesgo de manipulación indebida de equipos, información y medios informáticos.

Normas dirigidas a: funcionarios y directivos.

- Establecer una escala de sanciones para aquellos funcionarios que no cumplan las políticas de seguridad.
- Informar al área de sistemas cuando un funcionario ha cesado en su empleo.
- Cumplir con la aplicación de las políticas de seguridad establecidas en la empresa.

Normas dirigidas a: Oficina de Sistemas y Tecnología.

- Programar de manera permanente campañas y capacitaciones que sensibilicen a los funcionarios sobre la importancia de la seguridad de la información.
- Contar con mecanismos adecuados y seguros que permita el traslado, reutilización o eliminación de los equipos.
- Cancelar de inmediato las cuentas de acceso a los sistemas, cuando un funcionario ha sido retirado del cargo.

Políticas de seguridad física y del entorno

Áreas seguras.

Objetivo: Proteger los activos de la empresa contra amenazas físicas, humanas y del medio ambiente, evitando la interrupción del proceso productivo de la empresa.

Normas dirigidas a: Funcionarios y Directivos.

- Mantener las puertas de las oficinas cerradas, para evitar el ingreso de personas no autorizadas.
- Se debe gestionar la adopción de medidas adecuadas de protección física contra incendios u otra clase de amenaza.
- Se debe coordinar con la oficina de sistemas cuando se requiera realizar traslado de equipos entre dependencias, garantizando la protección del equipo y la información contenida.

Normas dirigidas a: oficina de sistemas.

- Realizar vigilancia permanente a las personas que ingresen cuarto técnico de comunicaciones.
- Verificar que las políticas de seguridad física se estén cumpliendo.
- Supervisar que los equipos informáticos estén en lugares libres de elementos inflamables y de todo tipo de riesgos de seguridad.
- Se debe implementar mecanismos de seguridad sin un funcionario de la empresa es reubicado con su respectivo equipo de cómputo.

Normas dirigidas a: personal de seguridad y vigilancia.

- Controlar el ingreso únicamente al personal autorizado.
- Deben llevarse un registro de visitantes que ingresen a la empresa.
- Efectuar registro diario del ingreso de portátiles o equipos tecnológicos ajenos a la empresa.

Seguridad en los equipos.

Objetivo: Conservar las medidas de protección adecuadas para mantener los equipos disponibles para las necesidades de servicio de la empresa.

Normas dirigidas a: oficina de sistemas.

- El equipo debe situarse en lugares alejados de todo tipo de amenazas externas.
- Mantener los equipos protegidos contra fallos en el suministro de energía, utilizando sistema de alimentación ininterrumpida (UPS).
- Se debe proteger el cableado para evitar roturas o daños en el servicio.
- Programar mantenimientos preventivos a los equipos de cómputo.

Normas dirigidas a: funcionarios y directivos.

- La empresa debe gestionar la adquisición de plantas eléctricas para garantizar la continuidad del suministro eléctrico en caso de cortes imprevistos.
- No se debe sacar los equipos de cómputo fuera de las instalaciones de la empresa sin autorización de la oficina de sistemas.
- El buen uso de los equipos garantiza la permanente disponibilidad.