ARES

Revista Protección Integral

Edición 1 Nº 15 Mayo 2009
Quito - Ecuador - Sur América
http://www.ipc.org.ec/ares/

Seguridad Ciudadana

¿Cómo proteger a su empresa de una pandemia?

Seguridad Corporativa

Ofertas de trabajo que estafan

Recursos Humanos

Optimizar costos para Capacitar en tiempos de crisis

Suscríbase en línea en la siguiente dirección:
http://www.ipc.org.ec/phplist/

FUNDACIÓN IPC Integrated protection concepts
Creando Cultura de Seguridad

Índice

DIRECTOR
Ing. Kevin Palacios, CPP, PSP, CPOI
e-mail: kpalacios@ipc.org.ec

EDITOR
Lic. María Fernanda Torres
e-mail: ftorres@ipc.org.ec

COMITÉ EDITORIAL
Ing. Kevin Palacios, CPP, PSP, CPOI
Roberto Varas, CPP, CPO
Lic. María Fernanda Torres

DEPARTAMENTO COMERCIAL
info@ipc.org.ec

Maritza González
mgonzalez@ipc.org.ec

FUNDACIÓN IPC CONCEPTOS INTEGRADOS DE PROTECCIÓN

Av. Eloy Alfaro N 35 128 y Portugal
Quito – Ecuador – Sudamérica

Tel: (593 9) 9 5417 322
Fax: (593 2) 2275 075
info@ipc.org.ec

www.ipc.org.ec

TIRAJE: 38. 265 suscriptores
12 países

DISTRIBUCIÓN GRATUITA

Una organización del Grupo:

PROSEC INTERNATIONAL
Hacemos del Mundo un lugar más Seguro

5 MINUTOS PARA HABLAR DE SEGURIDAD

SEGURIDAD INDUSTRIAL

LAS BROMAS PESADAS SON PELIGROSAS

Desgraciadamente, dentro de nuestra organización tenemos también unos pocos caballeros andantes que bravamente arriesgan sus cuellos y los de sus vecinos todos los días. Pero aquellos caballeros antiguos tenían razón para hacer eso, querían un mundo mejor. Pero los que tenemos aquí solo lo hacen para lograr unas cuantas carcajadas.

Ya ustedes saben a qué clase de "caballeros" nos referimos. Para lograr una carcajada de los compañeros o ganarse una sonrisa de una chica se harán los tontos o tratarán de poner a otro en ridículo. Se acostumbra mucho molestar a los recién entrados. Se les hace toda clase de bromas para hacerles pagar la novatada. Eso es, en realidad, una cosa cruel. Casi todo empleado recién instalado en su trabajo está un poco confuso, todo es nuevo y raro para él, es fácil ridiculizarlo. Es el momento que necesita una mano guía, alguien que lo ayude. No sé de dónde algunos sacan cierto placer en bromear con la gente nueva.

Hay otros que gozan quitándole el asiento al compañero. Esto es muy peligroso, no solamente porque el perjudicado puede sufrir un golpe en el extremo inferior de la espalda que es muy sensible sino porque puede causar una reacción de parte del afectado que termine en tragedia para el más aventurado bromista.

Otros tienen el buen sentido de dejar sus bromas para las horas fuera del trabajo, pero lo hacen en los vestidores o en el baño. Luchan, se hacen cosquillas, con la mejor intención del mundo de divertirse un poco, pero olvidan que esto puede causar un resbalón, un golpe, que puede resultar en un brazo o una pierna partida.

Quienes dirigen el trabajo y tienen un sentido de seguridad no pueden aprovechar esta clase de diversiones, porque pueden traer muchas lesiones. Los trabajadores que tienen conciencia de seguridad no pueden recibir complacidos esta clase de juegos. Las bromas pesadas y la seguridad no se mezclan. La seguridad es un negocio muy serio, salva vidas y previene el sufrimiento, mientras que esa clase de bromas, esos juegos de manos, son de mal gusto e inseguros.

RECUERDE: juego de manos, juego de villanos

PROTECCIÓN FÍSICA

CAMINANDO EN LA CALLE

RECUERDE: El margen de seguridad entre el sospechoso agresivo y usted es de 20 metros.

Cuando el sospechoso esté cerrando el espacio entre ustedes (caminando en su dirección):

- Cruzar la calle y observe el comportamiento del sospechoso;
- Si el sospechoso cruza también, la probabilidad de que lo atacara pasa a ser mucho mayor;
- No permita que el Sospechoso "cierre el espacio", si eso ocurre usted no tendrá más nada que hacer, el Delincuente habrá "vencido".

Para no permitir el acercamiento o que el delincuente proceda a "Cerrar el Espacio":

- Busque un lugar para resguardarse, un local con muchas personas (bar o despensa) o un local con Guardias de Seguridad o Policías;
- Si no hubiere donde protegerse cambie el sentido de dirección (así usted mantiene el espacio entre ustedes dos);

El Delincuente está viniendo en su dirección

- De la vuelta y cambie de dirección, mantenga el espacio entre usted y él.

El apresuró el paso hacia su dirección

Procure un local seguro, con mucha gente/Guardias (tiendas, despensa, etc.).

No hay locales para protegerse

Corra y observe el comportamiento del sospechoso. Corra antes que se cierre el espacio entre ustedes, después del abordaje nunca corra!

Si el Delincuente corre en su dirección

Está claro que el pretende cometer un delito, siendo así Grite/Llame al 911 / #8.
Generalmente, el Delincuente no irá a correr detrás de usted por mucho tiempo ya el no quiere llamar la atención, prefiere escoger otra víctima menos preparada/atenta/PREVENIDA

¿Qué gritar?

Gritar **"socorro"** hace que las personas alrededor recurran, pues queda claro que hay peligro.
Gritar **"fuego"** podría despertar el interés de las personas, haciéndolas salir de las casas para ver donde está el fuego.
Gritar el nombre de alguien**, "Jorge!"** es la mejor opción, el Delincuente creará mucha atención y podría presumir que hay más personas en el entorno/local (¿quién es Jorge, un hombre, un policía, un perro feroz?).
REGLA:
Si tuviere el "presentimiento" de que alguien va a abordarle **"nunca deseche la posibilidad".** Muchas personas que fueron asaltadas relatan que percibieron que algo iba a ocurrir y no realizaron la Prevención.

COMO PROTEGER A SU EMPRESA DE UNA PANDEMIA

Muy seria ha sido la crisis que se ha originado con respecto a la salud, producto de la gripe tipo A que se originó como se sabe desde México, hasta el extremo que ya se encuentra en nivel 5 de alerta (el segundo más alto), ya ha llegado a otros países como los estados unidos, algunos de Europa, Latinoamérica, Centroamérica, China. Desde luego alarma las muertes, por contaminación que ello ha originado y ha hecho que los gobiernos le presten atención a su desarrollo a fin de tomar las precauciones preventivas que eviten mortandad, contaminación masiva., como muchos lo han hecho y lo han logrado.
En el análisis realizado en su Boletín, Universia-Knowledge@Wharton, se comentan, que el 73% de las empresas de todo el mundo reconoce no tener ningún plan de contingencia para afrontar una pandemia de gripe, según datos de la consultora de riesgos Marsh. En un año sin contratiempos, las empresas pierden alrededor de 210 millones de euros anuales por culpa del absentismo, cifra que podría llegar a multiplicarse por tres en caso de pandemia. Si, además ésta se prolongase mucho en el tiempo, el absentismo laboral podría rebasar el 50% de la plantilla. Juan García Gay, responsable de Consultoría en Continuidad de Negocio de Marsh, explica que una gripe como la de tipo A, que ya se encuentra en nivel 5 de alerta (el segundo más alto), tiene un doble impacto, ya que no sólo dispara el absentismo laboral, sino que también tiene un efecto psicológico en la plantilla de la empresa, que tiene miedo de contagiarse e incluso puede vivir un drama en su entorno familiar.
Durante la crisis de 2006, cuando el riesgo de pandemia era inminente, algunas empresas se interesaron por mejorar su preparación ante eventos de este tipo. Sin embargo, en el momento que el problema fue perdiendo actualidad, muchas olvidaron de que siguen sin estar preparadas para el riesgo de un brote pandémico. No cabe la menor duda que es muy cierto que muchas empresas deben haberse resentido en su productividad, eficiencia con el absentismo, ante una amenaza seria, como en el caso de México en donde más la crisis se acentuó. Ello debe obligar a la gerencia, sus recursos humanos a tener planes de contingencias que afronten estas situaciones para no sufrir pérdidas en sus beneficios. Una buena gerencia debe prever los hechos y no esperar que se presenten, con ello se evita el deterioramiento en la operatividad eficaz de la empresa, en su productividad. La fiebre española de 1918 se cobró alrededor de 30 millones de muertes, y pandemias similares se repitieron en 1957 y 1968, aunque su mortalidad fue diez veces menor. La crisis del SARS (Síndrome Respiratorio Agudo Severo) fue un primer aviso del riesgo de un contagio mundial. Este episodio supuso un coste de 40.000 millones de dólares en las economías de Asia Pacífico, donde se contagiaron 8.000 personas. De tratarse de una auténtica pandemia, éste sería el número de personas que se infectarían cada hora.

En México, por ejemplo, se han agotado las mascarillas y la demanda de antivirales se ha disparado. Especialistas consideran que no es necesario realizar acopio de material sanitario sin valorar las necesidades auténticas, como, por ejemplo, cuántas personas podrán trabajar desde su casa y cuál es el personal necesario para mantener las actividades fundamentales. Las grandes compañías, que disponen de medios y personal cualificado, pueden almacenar desde antivirales hasta desinfectantes, mientras que otras firmas sin capacidad pueden llegar a acuerdos con laboratorios y proveedores sanitarios para que les sirvan de forma preferente o incluso les guarden el material que adquieran.

Revisar la política de viajes, atender las recomendaciones de la OMS o informarse de si el seguro de la compañía cubre este tipo de contingencias son algunas de las recomendaciones de los expertos. Muy interesante y valiosa la aportación cuando se indica, que los aspectos clave que debería considerar toda empresa son:

1. Revisar la política de viajes de la compañía, sus políticas de higiene y sus políticas sanitarias (revisiones médicas a los empleados), así como el número de antivirales disponibles y de otros cuidados médicos, tales como desinfectantes antibacterianos, mascarillas y otros materiales.

2. Tener claro si existe alguna distancia interpersonal recomendada u otras medidas que ayuden a minimizar la propagación del virus en el lugar de trabajo.3. Revisar los métodos actuales para informar a los empleados de la amenaza pandémica y de la situación actual del negocio, tanto si están en la oficina como si trabajan desde casa.4. En centros de población, estar seguros de que los planes previstos contemplan que el personal pueda trabajar desde casa cuando sea posible y apropiado.5. Considerar si existen procesos clave que debieran ser mantenidos en caso de que estalle una pandemia, tales como call centers, los servicios médicos de la compañía y otros servicios vitales e imprescindibles.

6. Revisar la estructura necesaria para gestionar de forma efectiva una posible crisis, y revisar cómo implementar varios planes de continuidad de negocio, cómo arreglárselas en caso de que se incremente el número de empleados que tienen que trabajar desde casa y cómo reaccionar ante

cambios importantes en nuestra cadena de suministro y en el mercado.

7. Asegurarse de que los planes de gestión de crisis y de continuidad de Negocio incluyen escenarios pandémicos y ejercicios para ensayar el plan cuando sea posible. Además del acopio de material sanitario y la revisión de procesos, los planes de contingencia tienen que tener en cuenta los mecanismos de comunicación, tanto con los empleados como con las Autoridades Sanitarias. Especialistas en el área de manejo de crisis sostienen que la colaboración con los organismos públicos de salud garantiza que la cadena de res puesta pública funcione correctamente.

Los Ministerios de Salud Pública, Agricultura y Ganaderia, Ambiente, Servicio Ecuatoriano de Sanidad Agropecuaria -SESA, OPS, OMS, FAO, en el 2005, en el contexto de la Pandemia de Gripe aviar, desarrollaron el **Plan de Contingencia para enfrentar posible pandemia de Influenza,** ya activado, contempla fortalecer los preparativos para una padema e influenza a escala mundial, regional, nacional e infranacional; reducir al mínimo el riesgo de transmisión a los seres humanos; detectar y notificar rápidamente la transmisión, cuando ocurra. De cualquier manera, cada compañía debe sumar a dicho plan nacional su propio mecanismo de respuesta con medidas propias que ayuden a evitar el contagio y minimizar las consecuencias de la epidemia.

Fuente:
Boletín de Universia-Knowledge@Wharton. wharton@universia.net
http://74.125.45.132/search?q=cache:U8dfdh8ebNkJ:www.opsecu.org/imagenes/uploads/File/Plan%2520Nacional%2520Influenza%2520Aviar.pdf+plan+de+manejo+de+pandemias+ecuador&cd=1&hl=es&ct=clnk&gl=ec

FUNDACIÓN

IPC | Integrated protection concepts

Creando Cultura de Seguridad

Una empresa del Grupo PROSEC INTERNATIONAL

Cumpla sus obligaciones de Capacitar...

en Seguridad y Salud Ocupacional
a Comités Paritarios y Brigadas
sin mayores complicaciones

Curso de especialización en Seguridad y Salud Ocupacional

Para Comités paritarios y brigadistas

Resolución CISHT # 013/06/12

Capacitación Modular Semi-Presencial

Inicio: 30 de Mayo, 2009

MODULOS

1. Conceptos básicos de seguridad y salud en el trabajo.
2. Riesgos generales y su prevención.
3. Actuación en emergencias.
4. Elementos de gestión en seguridad y salud ocupacional.

Informes e Inscripciones: 292 3600 ext 122 -124 | 098 104457
info@ipc.org.ec

Resolución 013/06/12

Member

ISO 9001

Pacificar Conflictos en Áreas Públicas

Por: Tibor Zsámboki
Experto en Seguridad Física

Enseñar técnicas de seguridad física a agentes de seguridad es un tema bastante complejo y requiere mucha responsabilidad.

Tanto en la antigüedad el Samurai y su adversario el Ninja, como en la época moderna los comandos de las fuerzas especiales aplicaron técnicas de manos libres basadas en diferentes Artes Marciales para complementar con sus armas. Con su aplicación en casos específicos lograron introducir sus armas en el combate u obtener la ventaja cuando estaban desarmados.

El objetivo siempre era lo mismo: eliminar el enemigo en combate cercano. Sin embargo, esto cambio en las guerras modernas que se pelean en terrenos inhóspitos, como la selva. La nueva táctica es infligir un daño permanente en las piernas porque así sacan mínimo tres soldados más fuera de combate quienes tienen que cargar el compañero herido.

Para escoger la táctica y los conceptos que enseñar siempre hay que tomar en cuenta los objetivos del grupo o individuo que participan en el curso.

En **áreas públicas** es muy importante evitar daños a terceros. Muchas empresas solucionan este problema de manera muy fácil y conveniente: no les dan armas a sus agentes en vez de enseñarles cómo manejarlas y cómo proceder.

Eso hace muy vulnerable el objeto protegido. Pues por la ley del Menor Esfuerzo y Mayor Resultado se vuelven blanco fácil para los asaltos, sobre todo cuando se unen otros factores, como acceso fácil a vías rápidas de escape, etc.

También es importante proceder con firmeza pero sin hacer daño, cuado se trata de usuarios que cometen alguna infracción. Si esto no sucede, la empresa puede enfrentar demandas o producir espectáculos tristes y desdichados para el público presente.

Enseñar cualquier Arte Marcial en general a los agentes, también puede ser un grave error, aún mas cuando es una disciplina deportiva. Dura años para masterar si no toda la vida y fácil pueden caer en la aplicación de fuerza excesiva. Cuando Gautama Buddha enseño a sus discípulos, tomo un puñado de hojas en su mano y señalo: Esto es lo que estoy enseñando a ustedes, porque solo esto necesitan para llegar a la iluminación, pero miren cuantas hojas hay en este bosque.

A los agentes hay que enseñarles técnicas sencillas, fáciles de aprender y aplicar, que funcionen para todos y contra todos. Tiene que ser reducidos en número. En caso contrario causa confusión y demora en su aplicación.

Más allá de la técnica y la táctica importa la mística. Si esta falla el resto no sirve de nada. Por eso la preparación psicológica valida el resto de materias. La actitud determina todo. No es el mejor agente quien mejor aplica las técnicas en su trabajo sino quien nunca necesita aplicarlas. Esto es el Concepto de Combate no Combate de mi Arte Marcial, Lotus Ryu Ju-Jitsu que consiste en desarrollar una presencia, campo energético tan fuerte que cualquier agresor potencial desiste de su ataque.

El conocimiento de la Tecnología de "El Centro" le convierte al individuo prácticamente invencible. Del Código Samurai se aprende a dar lo mejor de si en cada momento. Aprendiendo a desarrollar y a usar la intuición previene a cualquier imprevisto.

La suma de todo esto resulta en una actitud segura de si misma, predisposición total y estado de alerta que repele cualquier intensión maliciosa.

Fundación IPC

Próximamente realizará un curso practico:

"Defensa Personal y Pacificación de Conflictos en la Atención a Ciientes"

Para pre-inscribirse contáctenos a info@ipc.org.ec

CERTIFICACIÓN PARA OFICIALES BÁSICO DE SEGURIDAD PRIVADA -BPSO-

Curso Teórico-Práctico

DIRIGIDO A
Operadores de Seguridad Básicos
Dirigido a todo público que se inicia en la protección

Curso para Empresas e Industrial

Con el respaldo Académico de la Fundación Internacional para Oficiales en Protección -IFPO-

IFPO Internationa Foundation for Protection Officers

Financiamiento del 80% al 95% a través del

CENTRO DE CAPACITACION CNCF ACREDITADO Res. No. Vigencia

Consejo Nacional de Capacitación -CNCF-

CONTÁCTENOS
Maritza González
E-mail: mgonzalez@ipc.org.ec
Telf: (593 2)2923 600 | ext.122-124

Por qué las personas crean virus

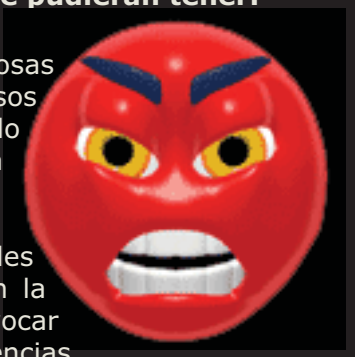
La imagen de desarrolladores de virus es de niños inteligentes con demasiado tiempo en sus manos y con el recurso de la tecnología digital para entretenerse. Pero ... ¿por qué las personas crean virus?

La respuesta no es tan simple como se pensaría. Hace años, la hipótesis de por qué la gente desarrollaba virus tuvo una explicación un poco más exacta, sin embargo, los tiempos han evolucionado y los creadores de virus y otros códigos maliciosos tienen muchas otras razones que sería difícil priorizarlas.

Hay muchísimas formas de contagiarse por un virus o amenaza, es vital que para proteger nuestros sistemas empecemos a dejar de lado la ignorancia y ampliar nuestros conocimientos sobre este tema, es importante reconocer que no solo se trata del riesgo de la PC, sino suyo propio, pues, los daños en muchos casos afectan económicamente.

Sin embargo, por qué las personas crean o desarrollan virus o sistemas maliciosos No se sabe a ciencia cierta el porqué, solamente sus creadores lo saben. Muchas personas crean virus para que lleguen a ser famosos, otras por el simple hecho de hacer daño o también para obtener un beneficio económico, robando contraseñas, cuantas

No se puede saber por qué estas personas, "cracker", desarrollan códigos maliciosos, sin embargo se pueden hacer algunas generalizaciones sobre las razones que pudieran tener:



Cuestiones Enojo: Hay quienes, por cualquier razón, simplemente hacer cosas destructivas para la causa de su destrucción. Pueden ser narcisistas maliciosos psicópatas o, simplemente, de manera egoísta en su impresión de que el mundo entero está en contra de ellos que azotan ciegamente a cabo en todos y cada uno cuando llegue la oportunidad por la causa de su destrucción.

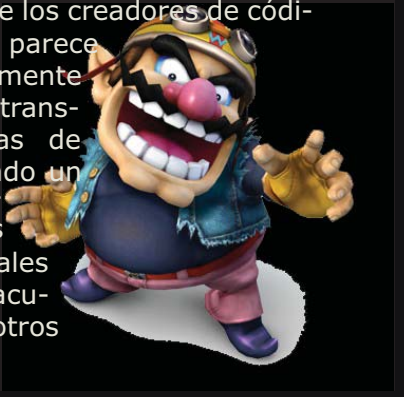
Hacerlo por diversión: algunos todavía lo hacen por la "diversión" que les conlleva generar cierto caos. Pueden sentir emoción al leer o escuchar en la prensa sobre los problemas que causa a las personas su trabajo o pueden provocar un "incendio" duplicando programas destructivos, sin considerar las consecuencias de sus actos.

Espionaje: No hay que confundir con sabotaje, de eso se hablará más tarde. Por "espionaje", nos referimos a los intentos de obtener información a través de medios fraudulento, debido a razones que identifican al fraude de identidad y otros, directa y penalmente lucrativas. Virus, gusanos, troyanos, e incluso accesos posteriores y otros programas malintencionados, colados en su software por el vendedor puede servir para propósitos de espionaje.

Las pandillas en línea: Probablemente suena como el betseller de ficción de Bruce Sterling "Islas en la red", escrito en 1980, pero este podría convertirse en realidad. Existen "pandillas" que utilizan a niños para que participen en actos de vandalismo digital como parte de un mal deseo de mejorar la identidad de grupo y de orgullo personal el convertirse en rebelde, o miembro de la comunidad "underground".

El Instinto de Hacker: Tenga en cuenta la diferencia entre un hacker y un cracker de seguridad. Con esto en mente, las personas con mentalidad de un hacker por lo general se encuentran desarrollando áreas específicas de interés en sistemas. En algunos casos, este interés puede girar en torno a la comprensión de códigos maliciosos de auto duplicación y a veces, la mejor manera de probar algo que ha creado es ver como opera bajo condiciones del mundo real. Algunos piratas informáticos inmorales o amorales con interés en códigos maliciosos de auto duplicación pueden probar su creación liberándolo y ver como trabaja

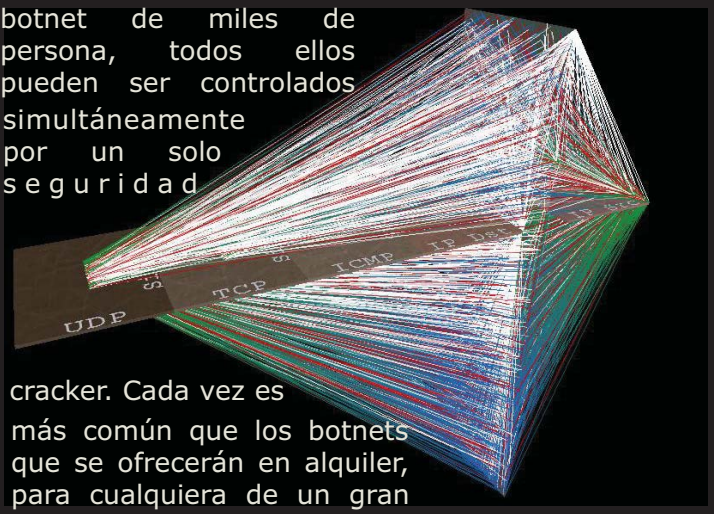
Dinero, dinero, dinero: La mayoría de los creadores de códigos maliciosos en la red, en estos días parece que entran en esta categoría, únicamente por lucrar. Virus y gusanos a menudo transportar cargas útiles que abren vías de intrusión en un sistema, proporcionando un medio para "cockies", ya sea de seguridad o de herramientas automatizadas para pasar el sistema de defensas. Tales herramientas automatizadas pueden acumular información de autenticación y otros



bancarias, algunas otras por poner a prueba los productos de empresas de seguridad. Pero lo que si es seguro es que muchas personas crean virus por vanidad o presumir su creación "devastadora".

Da la impresión de que todos los males de Internet (virus, ataques a ordenadores, robos de tarjetas de crédito, etc.) son obra de los 'hackers'. Su nombre aparece relacionado con la mayoría de las acciones fraudulentas de la Red, aunque la realidad es muy distinta: su actividad no tiene por qué ser malintencionada ni pretender producir daños. Un 'hacker' es una persona que sólo desea conocer el funcionamiento interno de los sistemas informáticos, ayudando a mejorarlos en el caso de que detecte fallos en su seguridad. Sin embargo, un 'hacker' deja de serlo cuando provoca daños y su acción es malintencionada: en ese momento pasa a ser un 'cracker'.

datos, aparecen como generadores de "spam" automáticos, o le ponen en contacto con un mecanismo centralizado de control de algún tipo, como una sala de chat de IRC para crear un botnet de miles de persona, todos ellos pueden ser controlados simultáneamente por un solo cracker. Cada vez es más común que los botnets que se ofrecerán en alquiler, para cualquiera de un gran número de razones.



Agitación Política: A veces, el vandalismo digital - ya sea por virus, gusano, ataque DDoS, o algunos otros medios - puede ser realizarse con el propósito de hacer una declaración o manifestación política. Si la razón es directamente política, en este sentido, es común que los programadores direccionen temas relacionados con el gobierno o políticas indirectas interfiriendo en ciertas clases de sitios Web y en algunas otras operaciones, el punto es que a veces las personas que no son directamente responsables suelen ser el blanco de la conciencia de la propia desaprobación de esos objetivos. Ataques como DDoS contra Microsoft o Yahoo! pueden caer en esta categoría.

Sabotaje: Algunas veces el propósito de códigos maliciosos puede estar directamente enfocado a interrumpir las operaciones de algunas clases de personas que nos les agradan. Si bien este tipo de comportamiento podría parecer superficialmente similar al "terrorismo", o vandalismo como se describió con anterioridad, este no es terrorismo y es mucho más personal que un típico vandalismo. Este es un acto criminal, dirigido a un objetivo específico, más afín a un asalto. Las personas con intereses en negocios pueden realizarlo sin ánimo de lucro o con fines políticos, pero los daños a otras empresas se centran en la incapacidad para competir, al menos temporalmente. Las agencias gubernamentales pueden hacer esto para tratar de intimidar a otros gobiernos para que estos hagan algo que no desean hacer, como se sospecha sucedió en el caso de Guerra cibernética estonio.

LUZ SOLAR EN OFICINAS

¿Cómo hacer frente al deslumbramiento?

En cualquier oficina moderna, el trabajo realizado por una persona involucra, entre otros aspectos, la rápida identificación de los tipos del teclado del computador y la lectura de lo que se está digitando. Por esta misma razón debe existir una estrecha relación entre la contribución de luz solar en un espacio interior y la generación de ésta por parte de la pantalla de un computador, de modo de propiciar un trabajo eficiente, sin producir el nocivo deslumbramiento, que dificulta la visión por parte del trabajador.

Asimismo, la ubicación de una persona en su puesto de trabajo debiera diseñarse según la relación de las fenestraciones y la orientación solar del recinto. La luz solar incidente controlada por

una persiana manual es un potencial de intervención desde el interior del espacio habitable.

En este contexto, una edificación debiera idealmente comprenderse como una suerte de envolvente que filtra y pone en sintonía las condiciones climáticas exteriores con las condiciones ambientales interiores.

Así como la piel humana, la envolvente de un edificio debiera considerar las condiciones climáticas, geográficas y urbanas para ser eficiente.

El efecto de la iluminación natural depende de las proporciones del espacio interior y de la cantidad, tamaño, ubicación y forma de las fenestraciones o aperturas por donde penetra la luz solar. En este sentido, algunas recomendaciones de diseño:

- Techos de gran altura, de formas alargadas y con aberturas en los planos laterales, facilitan una penetración efectiva de la luz natural.

- Diseño de plantas libres con pocas divisiones interiores o translúcidas favorecen la contribución de la luz natural, lo cual es muy importante en el caso del diseño de oficinas.

Las proporciones de un espacio interior tienen una especial importancia en la penetración de la luz. Así, hay que pensar que para iluminar con luz natural un espacio de largo interior 4.5 metros, la altura mínima de la fenestración deberá ser de unos 2.4 metros desde el nivel de piso.

Si la profundidad del recinto en relación a su ventanal es de entre 4.5 y 10.0 metros, por ejemplo, se necesitará el aporte de la luz eléctrica para mejorar la iluminación. Más allá de los 9.0 metros, la luz eléctrica suministrará la mayor parte de la iluminación.

Otro dato importante de tener en cuenta son los colores. Los claros y brillantes reflejan mejor la luz incidente, pero deben usarse cuidadosamente para evitar el deslumbramiento que puede llegar a ser muy molesto. Las superficies claras y mates, por otro lado, reflejan y difunden la luz, originando ambientes más controlados y homogéneos, por lo tanto más idóneos para el trabajo.

El nivel de iluminación sobre la superficie de trabajo proviene directamente de las fuentes luminosas (luz natural y/o artificial) y de las múltiples reflexiones en techo paredes y pisos. Según el color de las superficies, se puede aumentar la reflectividad y lograr un ahorro aproximado del 15% de la energía consumida en sistemas de iluminación artificial.

Finalmente, así como existen normas que regulan la emisión de luz contaminante al hemisferio superior, también debiera comenzar a regularse la redistribución de la luz solar en el espacio habitable tanto exterior como interior del hombre moderno. De esta forma tendríamos una mejor calidad de vida, un ahorro energético, y en armonía con la sustentabilidad del planeta.

Fuente:
Compatibilizar luz solar y artificial en la oficina, Fox,Alan docente de la Escuela de Diseño de la Universidad Andrés Bello.

FUNDACIÓN

IPC | Integrated protection concepts

Creando Cultura de Seguridad

IFPO

Obtenga la Certificación profesional más aceptada en el mundo de la seguridad y protección

Certificación Internacional Oficial Certificado en Protección -CPO-

Metodología a distancia y semipresencial

Informes e incripciones

Maritza González

E-mail: mgonzález@ipc.org.ec

Telf: (593 2) 2923 600 | 601, ext. 124

QUITO -ECUADOR

Existe algunas estrategias de capacitación que le permitirán seguir capacitando a su personal con éxito

La mayoría de las organizaciones destinan un monto significativo de esfuerzo a acciones de capacitación, tanto internas como externas. Ello radica en el simple hecho que la capacitación ha sido tradicionalmente definida como una forma de transferir conocimientos, habilidades y destrezas hacia las personas que se desempeñan en las organizaciones y a fortalecer actitudes necesarias para el éxito del negocio, sin embargo, la crisis empieza a dejar su huella. Las políticas de ahorro de costos, como formar instructores internos y eliminar gastos superfluos, apuntan a continuar con el entrenamiento del personal.

Lo cierto es que las compañías se esforzaron por optimizar recursos. Estrategias tenemos por ejemplo, la utilización de instructores internos; contratación de proveedores locales; financiación conjunta, entre empresa y empleado, de cursos externos; y reducción de gastos superfluos (alquiler de salas, hoteles, almuerzos, refrigerios y viajes).

Optimizar costos para Capacitar en tiempos de crisis

Así, la transnacional Xerox, a partir de 2001, adoptó una política de reducción de costos general que se extendió al presupuesto de capacitación. Con el objetivo de utilizar los recursos propios y reducir los contratos externos, la compañía implementó un programa de capacitación por medio de "facilitadores": un grupo de empleados de diferentes áreas que fueron seleccionados y preparados para entrenar al personal.

Otra opción para aprovechar al máximo los recursos internos fue la adopción del **e-learning**, un programa por el cual los empleados pueden acceder sin costo, a través de la intranet, a cursos técnicos, de habilidades generales y de negocio. Estas técnicas o estrategias son una manera de continuar dando entrenamiento sin interrumpir totalmente la capacitación.

Otra estrategia es maximizar el presupuesto de capacitación, es decir, trabajar intensamente para optimizar recursos y, de esta manera, dar continuidad a todos los programas clave de la compañía, de esta manera el objetivo de la compañía será no malgastar el dinero en actividades que no sean centrales ni agreguen valor al negocio. Así, si para los cursos gerenciales, de liderazgo, negociación o presentaciones efectivas antes las actividades se hacían afuera, en un hotel, lo que incluía el costo de comidas y traslados. Ahora, las actividades se hacen en la compañía y utilizando el comedor.

Imagine lo que empresas pequeñas tienen que recortar para no ver afectadas sus economías cuando grandes transnacionales se han visto afectadas por la crisis y con ello a suspender cursos. En el 2001, la industria Bayer, mantuvo, por entonces únicamente los cursos de estricta necesidad, como los vinculados a un proyecto de informática, y técnicos de fábrica sobre procedimientos productivos, similar situación la tuvo ARCOR quienes adoptaron medidas de optimización de costos, como la implementación de cursos con instructores internos, acuerdos de honorarios con proveedores, capacitación a través de e-learning y ahorros en costos indirectos.

¿CÓMO INVERTIR MEJOR EN CAPACITACIÓN? ¿CÓMO MEDIR EL RETORNO DE ESA INVERSIÓN?

Es difícil determinar desde un aspecto económico-financiero cuánto de lo invertido retorna al negocio. Sin embargo, existen hoy instrumentos de medición que permiten evaluar en términos cualitativos los impactos de adquirir nuevas capacidades y potenciar el capital intelectual.

¿La capacitación está orientada a un desempeño superior? ¿Está orientada a resultados? ¿Tiende a optimizar recursos y tiempos? ¿Motiva a las personas a tener un espíritu innovador y de mejora continua?

La evaluación como fin de monitorear los progresos alcanzados por los participantes en el aprendizaje, la integración de conocimientos con habilidades y su posterior aplicación en el desempeño cotidiano es el desafío de toda área de Recursos Humanos.

En síntesis, un proceso de capacitación puede medirse en aspectos cualitativos si existen objetivos claros y específicos. Potenciar y apalancar el factor humano como llave de la capacidad competitiva en el desempeño organizacional debe formar parte de cualquier Plan Estratégico que esté orientado a conquistar y mantener mercados, innovar y adaptarse de forma permanente y maximizar los resultados del negocio.

Fuente:
Optimizar recursos para capacitación, PERNAS, MARIANA
http://www.materiabiz.com/mbz/capitalhumano/nota.vsp?nid=28252

Curso Compacto

Conducción Evasiva-Defensiva

Certificación emitida por la Fundación IPC
con aprobación del
Ministerio Nacional de Educación,
aval de I.B.S.S.A y National Safety Counsil

Forme parte del entrenamiento completo para prevenir accidentes y reaccionar adecuadamente ante intentos de robo, secuestros o atentados

18 horas de capacitación teórica y práctica en conducción segura

DIRIGIDO A:

Protectores y Conductores para Ejecutivos
Conductores de vehículos empresariales
Gerentes y Ejecutivos, y
Público en General interesado en sus seguridad

INCLUYE

- Certificación Internacional de NATIONAL SAFETY COUNCIL -NSC-
- Certificación de la Fundación IPC, avalada por IBSSA
- Guías de curso (Conducción defensiva)
- Curso de acuerdo al contenido escogido
- Uso de vehículos para pruebas prácticas (Conducción evasiva)

CON EL RESPALDO DE

CISHT

Resolución 013/06/12

CURSOS IN COMPANY

CONTÁCTENOS

Fundación IPC
E-mail: info@ipc.org.ec
Telf; (593 2)
2923 600|ext.122-124
Cel: 09 8 104 457

Estafan con ofrecimientos de trabajos desde la casa

Una nueva demanda por fraude de la Comisión Federal de Comercio (FTC) contra una empresa que ofrecía ganancias a hispanos por trabajar desde la casa pone en evidencia la necesidad de mantenerse alerta ante este tipo de estafas

La FTC presentó cargos ayer contra la empresa "International Marketing", con sede en Puerto Rico, y su propietario, Zoilo Cruz, por violar la ley al prometer falsamente a consumidores hispanos "ingresos sustanciales a cambio de una tarea de llenado de sobres".

De acuerdo con las autoridades, el demandado anunciaba la oferta laboral fraudulenta, que prometía ingresos de 1.400 dólares a cambio de un pago de una cuota de 37 dólares, en un sitio de Internet bilingüe y periódicos hispanos de Estados Unidos y Puerto Rico.

Tras el pago de la cuota, los consumidores recibían un folleto en inglés denominado "Incredible Home Mailing Program" en el que se les informaba que no se les pagaría por llenar sobres como se había expresado previamente y se les indicaba como repetir la estafa publicando anuncios para vender a otros consumidores el mismo panfleto, explicó la FTC.

A raíz de este nuevo caso de fraude, las autoridades alertan a los consumidores a ser cautelosos al momento de contemplar suscribirse a ofertas que prometen trabajo desde la casa a cambio de un "pequeño" cargo

DIARIO MI GENTE The Spanish Newspape.

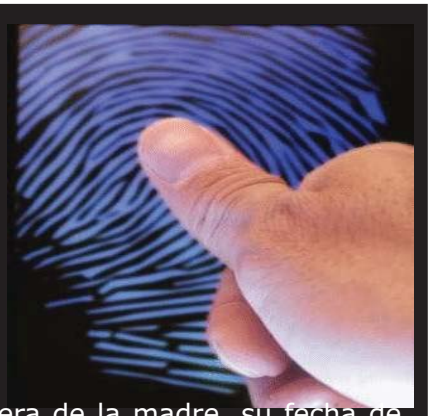
OFERTAS DE EMPLEO QUE ESTAFAN

Esta es una descripción de algunas de las estafas que más comúnmente se presentan a través del Internet o prensa

El reenvío de pago o transferencia de pago: En esta modalidad, el estafador pretende ser un empleador. Usa un anuncio o información de trabajo de un currículum vitae puesto por el aspirante en el Internet con el fin de convencerlo que es un empleador de verdad. Una vez que se ha ganado la confianza de la víctima, usa uno o varios planes para solicitarle su número de cuenta bancaria. Puede decirle que necesita entregarle su sueldo mediante "deposito directo" o prometerle un salario elevado por un empleo que incluye el reenvío, transferencia o envío de fondos de una cuenta personal bancaria, cuenta PayPal o de Western Union a otra cuenta. Se le dan instrucciones de que se quede con un pequeño porcentaje a cuenta de su sueldo (que puede ser desde cientos hasta miles de dólares). Regularmente el dinero que la victima transfiere es robado,

así que el candidato termina cometiendo un fraude por robo y transferencia de fondos.

La invitación "personal": Este tipo de estafas envía mensajes masivos a una larga lista de remitentes donde le afirman que han visto su currículum en el Internet, que cumple con los requisitos para el empleo y le invitan a llenar una solicitud de empleo en el Internet. También pueden decirle que ese mensaje es en respuesta a su solicitud de trabajo presentada por usted para cierto puesto. Sea cauto. ¿Se trata de un mensaje de un negocio desconocido o de alguna persona que usted no conoce? ¿Solicitó usted empleo en alguna organización? ¿Envió un currículum a algún reclutador de empleos? Anote y el nombre de la empresa, localícelo en el buscador del Internet y póngase en contacto telefónico con la empresa para verificarla.



Verificación de Identificaciones Personales: Durante el proceso de solicitud de empleo o antes de prometerle una entrevista personal, el estafador le dirá que para verificar su identidad, el negocio necesita escanear su licencia de manejar, su pasaporte u otro tipo de identificación. Tal vez que necesita los números de su cuenta bancaria o de su tarjeta de crédito para verificar su crédito antes de procesar su solicitud de empleo. Otra señal de alerta es cuando preguntan el nombre de soltera de la madre, su fecha de nacimiento o número de Seguro Social. Estas no son preguntas requeridas por ley y pueden utilizarlas para cometer algún robo de identidad.

Facilitarle la búsqueda de trabajos federales: Evite sitios de la red que mediante cierto pago prometan facilitarle la búsqueda de trabajos federales para obtener un empleo federal o en el servicio postal. Son muy dados a usar nombres parecidos a las agencies de gobierno tales como "U.S. Agency for Career Advancement" o el de "Postal Employment Service". Debe saber que es muy probable que le estén mintiendo al dar información sobre trabajos federales disponibles en su localidad, falsas oportunidades de trabajo en el gobierno federal que no han sido "reveladas", al prometer el pase "garantizado" a un determinado puesto o asegurar que recibirá un alto porcentaje en el examen de admisión para el servicio postal. Todos los puestos federales se anuncian públicamente y las agencias federales nunca le cobran al ir a solicitar empleo ni le garantizan la contratación de un solicitante.

RECOMENDACIONES

Al responder a un anuncio sobre un empleo o al llenar un contrato de colocación de empleo, antes de enviar dinero o información personal considere lo siguiente:

Esté consciente de que un empleador legítimo no necesita saber su número de cuenta para un "Depósito directo" antes de que usted se reporte para trabajar.

Verifique la confiabilidad de la firma y los récords de quejas con otros medios como BBB o en las oficinas de protección al consumidor.
Nunca divulgue información personal en el Internet a menos que haya verificado la confiabilidad de la empresa y su récord de trabajo, que sea seguro el medio de transmisión de información esté utilizando y que esté satisfecho con las políticas de protección de privacidad de esa empresa.

Existe una variedad de recursos disponibles con el fin de ayudarle en su búsqueda de empleo, que son gratuitos o a muy bajo costo, en los que se incluyen las oficinas de servicios de empleo de los gobierno estatales y locales, el Internet, las bibliotecas, universidades y colegios de la comunidad locales.

Fuente:
Consejo de Derechos de Autor de Better Business Bureaus, 2005. "Copyright Council of Better Business Bureaus, 2005".

Un Regalo de Vida

Herramienta de Rescate

RESQME

2 EN 1

CORTA-CINTURONES
ROMPE - CRISTALES

Salva Vidas en caso de choque o volcadura

INFORMES Y VENTAS

Info@ipc.org.ec
Tef: (+593 2) 2923 600 | 601 ext. 124
Quito - Ecuador

Cursos y Eventos

CRONOGRAMA CAPACITACIÓN 2009		
CURSO	**FECHA**	**LUGAR**
Certificación Internacional en Gerencia y Supervisión de la Protección –CSSM-	**Sistema Virtual Moodle** 20 de Junio	Visite la siguiente página http://www.ipc.org.ec/certificaciones/cssm.htm
Curso para Agentes de Básico de Seguridad con especialidad en Lugares Turísticos	**CURSO ABIERTO PARA EMPRESAS E INSTITUCIONES**	Visite la siguiente página http://www.ipc.org.ec/cursos
Conducción Evasiva – Defensiva (16 horas)	**CURSO ABIERTO PARA EMPRESAS E INSTITUCIONES**	Quito Visite la siguiente página http://www.ipc.org.ec/certificaciones/conduccion defensiva.htm
Curso Especializado en Seguridad y Salud Ocupacional -CSSO-	**CURSO ABIERTO PARA EMPRESAS E INSTITUCIONES**	Quito Visite la siguiente página http://www.ipc.org.ec/cursos.htm
Curso Brigadistas para el Manejo de Emergencias (16 horas)	**CURSO ABIERTO PARA EMPRESAS E INSTITUCIONES**	Visite la siguiente página http://www.ipc.org.ec/cursos

INFORMES Y VENTAS
Fundación Conceptos Integrados en Protección -IPC-
Av. Eloy Alfaro Nº35-144 y Portugal
E-mail: info@ipc.org.ec
Telf. (593 2) 2923 600 | 601 -ext. 124
Cel: 09 8 104 457
QUITO -ECUADOR