E-COMMERCE

SCP

SEO y SEM

Cyberoam

Avira

NEXXT SOLUTIONS

CRYPTOPHONE™

Cloud24x7

open source™

Índice

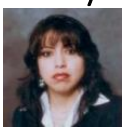
“.....”

– ..... –

CRÉDITOS:

Revista virtual de comercio electrónico, recopilación de los mejores artículos de la prensa internacional.

Recopilación y edición:



Consuelo de la Torre
c.delatorre@scprogress.com (+593 979003123)

Marco de la Torre
m.delatorre@scprogress.com (+593 998053611)

Editores Invitados:

Micaela de la Torre

Revisado por:

Arturo de la Torre

adltorre@scprogress.com (+593 999025294)

Síguenos en:

www.scprogress.com

Facebook

Twitter

¿Qué es el voto electrónico?

Nuestro país se encuentra a las puertas de que sus ciudadanos vuelvan a asistir a las urnas, para expresar su voluntad ante la consulta popular planteada por la Presidencia de la República del Ecuador, razón por la cual, SCProgress, presenta en esta ocasión, un análisis sobre los sistemas de votación electrónica, abarcaremos los temas más importantes relacionados con este tema, esperamos que sea de interés para nuestros lectores.

Existen varias definiciones para lo que se denomina comúnmente como “voto electrónico”. En un sentido amplio, se considera voto electrónico a la incorporación de recursos informáticos en cualquier parte del proceso electoral, ya sea en el registro de ciudadanos, la confección de mapas de distrito, la logística electoral, el ejercicio del voto en sí mismo, el escrutinio y la transmisión de resultados. Sin embargo, vamos a considerar estrictamente dos de las áreas del sufragio: la emisión del voto en sí misma y el recuento de votos.

En un sentido estricto denominaremos voto electrónico a los mecanismos diseñados para emitir y contar los sufragios en un único acto, a través de algún sistema informático instalado y en funcionamiento en el lugar mismo donde el elector concurre a expresar su voluntad política.

Entonces, entendemos por voto electrónico a todo sistema informatizado para el acto de emitir y contar los votos en la mesa de votación, donde los ciudadanos y las ciudadanas entran en contacto directo con los dispositivos electrónicos. Consideramos el uso de computadoras, urnas electrónicas o dispositivos similares para la emisión y recuento automatizado del sufragio. Los mecanismos en los que la computadora no está directamente involucrada en el acto de emisión del voto, así como aquellos que utilizan la informática exclusivamente para la automatización del recuento y la consolidación de resultados quedan así expresamente fuera de nuestra atención.

No existe una única forma de implementar voto electrónico, más bien podríamos decir que existen tres grandes tipos de sistemas a utilizar, que difieren no solo en su implementación, sino y fundamentalmente en sus riesgos y beneficios. Los mecanismos más frecuentemente identificados se pueden agrupar en tres grandes conjuntos:

a) Los sistemas de recuento automático de votos mediante reconocimiento óptico de las marcas hechas en la papeleta por parte de los ciudadanos (sistemas que hacen hincapié en el escrutinio electrónico);
b) Los sistemas de registro electrónico directo (red, o dre por su sigla en inglés) ejemplificados comúnmente con los denominados kioscos de votación o urnas electrónicas;
c) Los sistemas de votación a distancia a través de Internet.

FUENTES:

- https://blog.smaldone.com.ar/2017/03/26/que-es-el-voto-electronico/

SECaaS Security as a Service

SCProgress brinda el servicio más completo de seguridad informática optimizando los recursos y garantizando la Confidencialidad, Integridad y Disponibilidad de los sistemas.

FireSecure: El primer nivel de servicio que ofrece detalles de evaluaciones a los firewall, manejo de políticas de seguridad, verificaciones de cumplimiento de políticas, fortalecimiento de los Firewall, así como, políticas de remediación.
Con éste servicio se realiza una (1) auditoría por año.

SecurePlus: Una vez realizado el proceso de FireSecure, se brinda a los clientes el servicio SecurePlus, con el cual se ofrecerán reportes mensuales en los siguientes temas:

- Threat Intellicenge (Análisis de Amenazas)
- Breach Detection (Análisis de Vulnerabilidades)
- Event Correlation (Correlación de eventos)
- Incident Response (Respuesta a incidentes)
- Proactive Monitoring (Monitoreo constante de la seguridad de la plataforma)

Vulnerability Assessment & Pen Testing (Evaluación de Vulnerabilidades y Tests de Penetración): El nivel mas alto de evaluaciones de vulnerabilidades de los sistemas en toda la red, se elabora un informe detallado de test realizados y amenazas encontradas.

SCProgress recibe los mensajes automatizados del Centro de Operaciones en los casos de que exista detección de nuevas vulnerabilidades, ransom o amenazas, para coordinar las acciones a tomar con el cliente junto con el equipo de remediación (técnicos).

Inteligencia de amenazas

Alertas de seguridad en tiempo real

Administración de eventos y logs

Análisis y correlación de eventos

Monitoreo 24x7x365

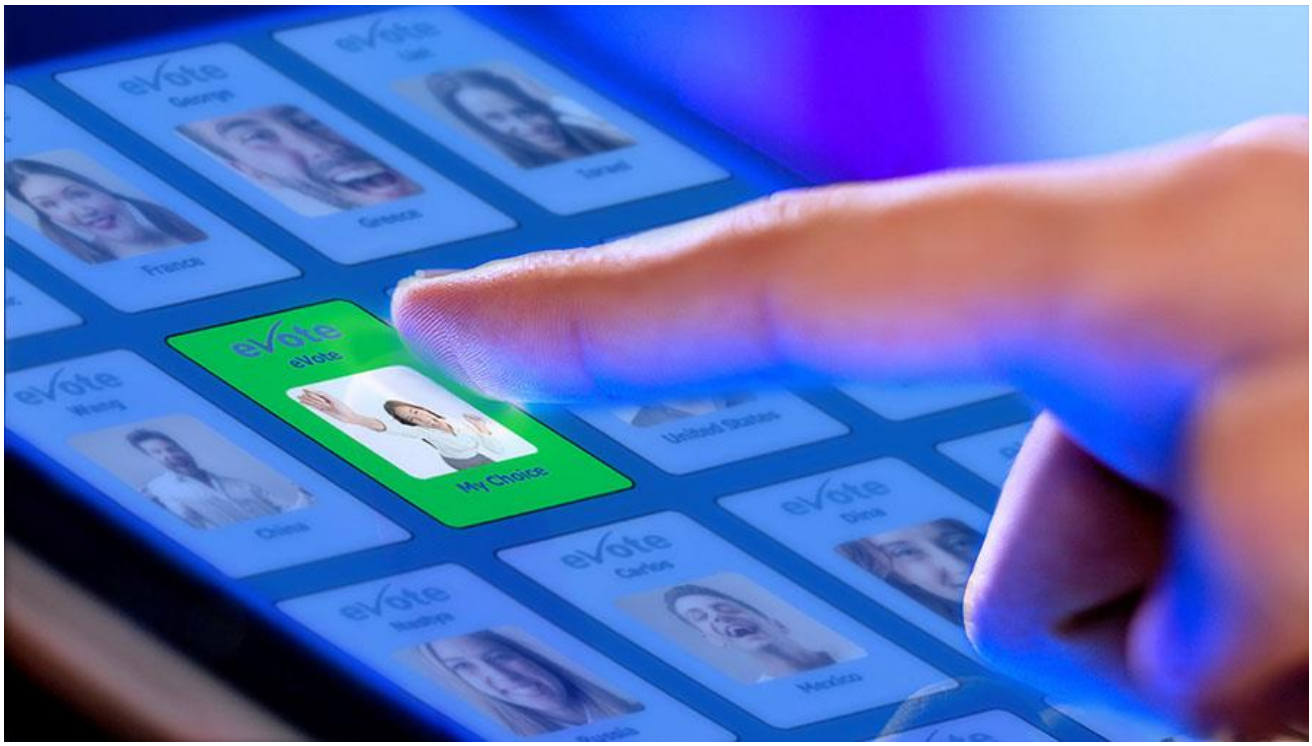
Gestión de respuesta a incidentes

Auditoría y solución de errores del firewall

VAPT

Gestión total del perímetro de seguridad

Sistemas más usados en el voto electrónico



Como se indicó en el artículo anterior, dentro del sistema del voto electrónico, existen varias versiones, SCProgress, pone a su consideración, de acuerdo a varios expertos en el tema, los sistemas más utilizados en los últimos años.

a. Sistemas de recuento automático

En principio, los sistemas de recuento automático resuelven el problema más álgido de la incorporación de tecnología al sufragio: al mantener el principio de que la voluntad del elector se expresa en un trozo de papel anónimo, desacopla el acto de emisión de voto (que debe ser inauditable) del acto de escrutinio (que debe ser auditable en todos sus detalles). De esta manera es posible construir un sistema en el cual todos los resultados en los que la informática está involucrada pueden ser auditados independientemente de los dispositivos usados y el software en sí, mediante el simple recurso de realizar un recuento manual.

Un elemento que no puede faltar en la aplicación de sistemas de recuento automático es la auditoría manual de los resultados arrojados por una porción estadísticamente significativa de las máquinas usadas, seleccionadas al azar luego del acto eleccionario. De lo contrario, una programación maliciosa del software de tabulación de votos podría alterar los resultados sin ser detectada.

Estos sistemas pierden una porción importante de sus ventajas cuando la papeleta no es marcada a mano por el elector. Las máquinas de marcar papeletas vuelven a introducir en el sistema muchos de los problemas asociados con las máquinas de registro directo. Si bien permiten que el votante verifique que las marcas en la

papeleta corresponda con sus elecciones, suponen un doble trabajo para el votante (elegir por un lado, controlar por otro), lo que aumenta la probabilidad de que el elector no realice concienzudamente el control. Esto hace factible el mismo ataque que se puede hacer en las máquinas de red: introducir código que intente adulterar la intención del votante, pero abandonar el intento si el votante rechaza la papeleta. De esta manera se pueden secuestrar los votos de todos aquellos ciudadanos que no sean lo suficientemente cuidadosos. También se pone en riesgo el anonimato del voto, toda vez que la máquina de marcar papeletas podría agregar, además de las manchas legítimas, algunas que pasen por "suciedad" pero que, en realidad, codifiquen información que permita reconstruir la secuencia de emisión de los votos.

Otro mecanismo que reduce la utilidad de estos dispositivos es el de pasar la papeleta por el escáner antes de introducirla en la urna, en vez de hacerlo al abrir esta. Esto no solo aumenta los costos –requiere un escáner por mesa, mientras que de otro modo puede utilizarse el mismo escáner para varias de ellas–, sino que potencialmente permite registrar la secuencia en la que se emitieron los votos, y así reconstruir la relación de cada votante con su voto.

Una crítica común es la que objeta la facilidad con la que se puede alterar o anular un voto mediante el agregado de marcas por parte de quienes realizan el escrutinio. Si bien la factibilidad del ataque es real, es exactamente la misma que con cualquier sistema basado en papel, que a su vez es mejor que la de cualquier sistema completamente electrónico: mientras que las papeletas pueden ser alteradas, esto debe ser hecho individualmente con cada papeleta, y el impacto de una persona corrupta se circunscribe a las papeletas bajo su custodia. En el sistema electrónico, en cambio, una única persona corrupta tiene el potencial de infectar un gran número de máquinas, comprometiendo de esa manera incluso la integridad de votos en masa, incluyendo los de mesas cuyos presidentes de las juntas electorales actúen de buena fe.

b. Sistemas de registro electrónico directo (red)

Los sistemas red o dre son aquellos que más se corresponden con el imaginario popular de las "urnas electrónicas". Representan, además, el modelo preferido de la mayoría de las empresas que participan de este mercado.

Los sistemas red se caracterizan por realizar simultáneamente el registro y la tabulación del voto mediante un dispositivo informático, operado directamente por el votante mediante un teclado, una botonera especial, o una pantalla táctil. Además, algunos sistemas de red ofrecen ayuda para personas con algún tipo de discapacidad, por ejemplo mediante una interfaz de audio para superar las dificultades visuales. A diferencia de los sistemas de recuento automático, en los que el soporte fundamental del voto es la papeleta marcada por el ciudadano, en las máquinas red el registro se realiza directamente en la memoria del dispositivo.

Muchos proveedores de equipamiento señalan como una ventaja del sistema el hecho de que permite "independizar del papel" a la elección. Por lo general, recomiendan no usar la opción ofrecida por algunos modelos de máquinas red de usar impresoras similares a las que funcionan dentro de las cajas registradoras para generar una cinta de auditoría, argumentando que "desnaturaliza el voto electrónico". En todo caso, las máquinas red no usan el papel emitido para

sus resultados, sino que se basan enteramente en los registros presentes en su memoria.

Los sistemas red pueden configurarse de tal modo que permitan al usuario corregir sus opciones y hasta votar en blanco, pero no permiten invalidar el voto ni cometer errores clásicos que resultan en la anulación del voto.

Por otro lado, estos sistemas suelen ser también los preferidos por aquellos que trabajan en las elecciones, porque son los que más trabajo ahorran: no hay papeletas que custodiar, el recuento de votos es inmediato, y no hay riesgo de que un nuevo recuento de votos arroje una diferencia con el anterior. La máquina obtendrá siempre el mismo resultado independientemente de si este refleja la voluntad de aquellos que la usaron para votar o no.

En esta preferencia, se hace evidente un punto de tensión entre los intereses de los ciudadanos (que necesitan que el resultado refleje sus elecciones) y los de quienes están encargados de conducirlo (que desean terminar la tarea con la mayor rapidez y el menor esfuerzo posible, descargando tanta responsabilidad como se pueda por eventuales errores o actos de corrupción).

c. Sistemas de votación a través de Internet

También conocidos como sistemas de votación a distancia, se trata de mecanismos para emitir el sufragio desde una computadora común conectada a la red de redes, permitiendo que los sufragantes emitan su voluntad desde sus propios domicilios, desde puntos públicos de acceso, e incluso desde el extranjero. Existen variantes de estos sistemas que permiten emitir el voto no solo desde una computadora personal, sino eventualmente también desde un teléfono celular o un sistema de televisión digital.

Uno de los desafíos más graves que enfrenta este tipo de sistemas es la identificación del votante, imprescindible para asegurar varias propiedades importantes del mecanismo, tales como evitar que alguien vote más de una vez o en nombre de otra persona, o que voten personas que no están habilitadas para hacerlo. Este problema suele resolverse mediante una clave unívoca y personal, que puede incluir elementos físicos de autenticación tales como la posesión de una tarjeta de identificación criptográfica o un generador de claves pseudoaleatorias.

Aun con los métodos de autenticación más sofisticados, no queda claro que puedan ser posibles reconciliarlos con los requerimientos de identificación exigidos por la ley, que por lo general requieren la verificación de documentos de identidad por parte de autoridades electorales.

Un problema adicional asociado al de la identificación es que estos sistemas obligan a que la máquina que recibe el voto tenga conocimiento de quién lo está emitiendo. Esto ofrece un punto único de ataque para quien quiera violar el secreto del voto: basta con obtener la información almacenada en el servidor del sistema de votos para averiguar cómo votó cada persona que lo usó.

Los defensores de estos sistemas señalan que se prestan a ser usados en lugares en los que la participación en las elecciones no es obligatoria y está permitido votar por correo. El argumento es sólido, en el sentido de que es un sistema que puede ser usado en contextos en los que la experiencia muestra que el riesgo de fraude es bajo.

Es interesante señalar que hay experiencias exitosas de uso de votación a distancia en ciertos ámbitos específicos, en particular en aquellos en los que los participantes tienen un grado alto de familiaridad y acceso a recursos informáticos y está ausente la exigencia de anonimato. El proyecto Debian, por ejemplo, un proyecto comunitario de desarrollo de software integrado por personas de todo el mundo que no tienen oportunidad de encontrarse físicamente para votar, utiliza voto a distancia como una herramienta cotidiana, con excelentes resultados. El sistema es robusto, justo y difícil de engañar, pero solo funciona gracias al hecho de que el voto no es secreto.

FUENTES:

- https://blog.smaldone.com.ar/2017/03/26/que-es-el-voto-electronico/
- http://codimi.edu.co/index.php/32-voto-electronico
- http://www.periodicodelbiencomun.com/propuestas-proyectos/el-voto-electronico-en-el-mundo-solo-7-paises-lo-usan/

Rincón de los Jóvenes

…….”

Principales problemas detectados en los sistemas de voto electrónico

Estos sistemas suelen venir de la mano de contundentes afirmaciones acerca de sus virtudes, tales como una mayor transparencia del acto electoral, la eliminación del clientelismo político, la rapidez e infalibilidad del conteo, el menor costo de cada elección, y la mayor participación ciudadana.

Lamentablemente, estas afirmaciones categóricas no vienen acompañadas de datos sólidos que las sustenten, y algunas empresas proveedoras invierten un esfuerzo nada despreciable en evitar que sean verificadas por terceras partes independientes, como fue el caso de Sequoia Systems en 2008, que intentó impedir una auditoría independiente de seguridad encomendada por el estado de Nueva Jersey argumentando que llevarla a cabo violaría los términos de uso del software que controla las urnas.

De hecho, ninguna de esas afirmaciones soporta un análisis profundo y, si bien algunas de ellas pueden ser ciertas para algunos casos particulares, la experiencia internacional demuestra que en la realidad están muy lejos de reflejar el verdadero desempeño de las urnas electrónicas. Detengámonos, entonces, en estas afirmaciones categóricas alrededor del voto electrónico.

1. La transparencia

La afirmación de que las urnas electrónicas aportan a la transparencia del comicio es, probablemente, la más aventurada. Es difícil comprender cómo un proceso opaco se haría más

transparente mediante el recurso de agregar una "caja negra". Lejos de aportar a la transparencia, la urna electrónica obstaculiza la capacidad de la mayoría de los ciudadanos de fiscalizar la elección.

Cualquier persona sabe cómo verificar, con solo mirar, que una urna está vacía o que un precinto de seguridad está intacto, y el sistema educativo apunta a garantizar que todas las personas sepan leer, escribir y contar. Pero estas habilidades son inútiles a la hora de ver qué pasa "dentro" de una urna electrónica: la inspección ocular no sirve para ver si está vacía sino que es necesario usar un programa diseñado a tal fin, que imprima un ticket que diga "sí, estoy vacía". La pregunta es: ¿Podemos creerle?

Cuando la urna imprime los resultados, los obtiene de operar sobre sus registros internos, almacenados en medios magnéticos que los fiscales no pueden leer por sus propios medios. La única "comprobación" posible de que la urna está

efectivamente vacía, o de que los totales son correctos, es repetir la operación, la que previsiblemente dará siempre el mismo resultado. Aun si confiáramos en que el programa de la urna es correcto, el fiscal promedio carece de los conocimientos y las herramientas necesarios para comprobar si el programa que está instalado en la urna ha sido adulterado o no.

Este es un problema fundamental de las urnas electrónicas: mientras la verificación de su confiabilidad dependa exclusivamente de comprobar que "funciona bien", la tarea de su fiscalización queda necesariamente en manos de una élite tecnológica, a la que el resto de la población no tiene más remedio que creerle. Para corromper la fiscalización de una elección basada en papel, es necesario contar con fiscales corruptos en un número importante de mesas, pero en el caso de las urnas electrónicas basta con sobornar o extorsionar a un grupo pequeño de personas fácilmente identificables.

Por lo demás, la afirmación de que estas urnas han sido usadas sin problemas es muy aventurada: no sabemos si hubo problemas o no, precisamente porque la opacidad del mecanismo no nos permite comprobarlo adecuadamente. Es perfectamente posible que en esas elecciones haya habido problemas masivos, sin que nadie haya podido probarlo y ese es precisamente el escenario que las urnas electrónicas facilitan.

2. El fin del clientelismo

El clientelismo político es un problema social, económico y educativo que no se soluciona con tecnología. Para que la "compra de votos" funcione, es necesario contar con un mecanismo que permita al comprador un grado importante de confianza en que el votante efectivamente votará por el candidato al que prometió votar. En las elecciones en papel, esto puede hacerse a través del denominado "voto en cadena", mecanismo que algunos sistemas de voto electrónico hacen efectivamente imposible.

Sin embargo, pensar que el voto en cadena y el clientelismo son lo mismo es un error: el voto en cadena es solo un mecanismo para romper el secreto del voto. No es el único, y las urnas electrónicas ofrecen mecanismos alternativos potencialmente mucho más eficaces. Esto se debe a la naturaleza fundamentalmente distinta de las urnas electrónicas. Por ejemplo, mientras que las urnas normales son contenedores pasivos de información, los circuitos de la urna electrónica emiten radiación electromagnética. Experimentos realizados en Holanda demostraron que estas emisiones hacían posible detectar por quién votaba una persona desde una distancia de 25 metros, usando solo dispositivos disponibles comercialmente.

Por ejemplo, en el estado de Ohio se descubrió, dos años después de usarlas, una grave falencia en las urnas electrónicas que permite violar el secreto del voto luego de los comicios: los reportes emitidos por la urna al final del recuento permiten reconstruir el vínculo entre voto y votante. Este caso es particularmente grave, porque ilustra un aspecto a menudo ignorado del cálculo de riesgo a la hora de usar una urna electrónica: el hecho de que no conozcamos vulnerabilidades en la urna no quiere decir que no existan, ni que nadie las conozca. Alguien que estuviera en conocimiento de esta vulnerabilidad hubiera podido organizar una compra o extorsión masiva de votos que hubiera sido indetectable y

requerido un esfuerzo logístico mucho menor que el voto en cadena.

3. La rapidez en el conteo

Una de las escasas ventajas promocionadas que podría ser verificable es la rapidez en el conteo. De hecho, cuando todo sale bien, los resultados pueden ser inmediatos. El problema surge cuando evaluamos el impacto potencial de las distintas cosas que pueden salir mal. Mientras que en la urna de papel, la influencia de un inconveniente es por lo general proporcional a la magnitud de este, en las urnas electrónicas un problema muy pequeño puede tener consecuencias muy graves. Esto lleva a que si los resultados de la urna electrónica no son inmediatos, por lo general no se los puede obtener nunca. Por lo general, no hay un punto medio.

El 16 de diciembre de 2007, por ejemplo, se utilizaron cuatro urnas electrónicas de la firma Altec Sociedad del Estado (Río Negro) en la localidad de Las Grutas, en Argentina. Transcurrida la jornada electoral, una de esas urnas arrojó un resultado sorprendente: 0 votos. Fue afortunado que, en este caso, las urnas hayan llevado registro en papel, porque el registro digital se había perdido completamente, pero aun así el escrutinio demoró horas, porque los votos impresos sobre una tira de papel eran mucho más difíciles de identificar que las papeletas originales. La única explicación de la empresa proveedora de la urna fue que “alguien debe haber sacudido la urna”.

De la misma manera, existen casos en los que una falla técnica en una urna electrónica produjo que la urna contara miles de votos en mesas en las que votaban solo cientos de personas, o el caso de Nueva Jersey, en el que los resultados fueron inmediatos, pero el total de votos emitidos no coincidía con la suma de los votos emitidos por partido. ¿Puede decirse que ese resultado es inmediato, cuando en realidad es evidentemente incorrecto?

La rapidez, sin confianza ni seguridad, no sirve para mucho en un proceso electoral. Esta es un área en la que la eficacia (hacerlo bien) debe primar por sobre la eficiencia (hacerlo rápido).

4. La economía

La idea de que usar urnas electrónicas permite economizar dinero en los comicios ha sido refutada por auditores independientes que la pusieron a prueba. En el estado de Maryland, por ejemplo, entre 2002 y 2003 se compraron 19 mil máquinas de pantalla táctil a la firma Diebold. Para poder concretar la compra, el Estado tomó un crédito de 67 millones de dólares, 44 de los cuales fueron a las arcas de la empresa en concepto de compra y mantenimiento de las urnas. Antes de incorporar estos dispositivos, Maryland usaba un sistema de escaneo óptico.

Según el informe de la organización Save Our Votes, publicado en febrero de 2008, el cambio de tecnologías implicó un aumento promedio de 179% en el costo total por votante. En uno de los condados, el aumento fue de 866%.

5. La participación ciudadana

Un tema crítico a la hora de evaluar la implementación de voto electrónico es la

participación ciudadana. Nuestras democracias modernas están golpeadas por el descrédito de las clases dirigentes y la falta de confianza en los sistemas políticos. El halo de modernidad que otorga el voto electrónico parece ser la panacea para entusiasmar a los votantes y alentar la participación en los comicios.

Sin embargo, es importante destacar que la incorporación de urnas electrónicas tiene efectos claramente contrarios al objetivo de mejorar la participación ciudadana. Sin ir más lejos, las personas poco afines con los sistemas computacionales serán los primeros excluidos: adultos mayores o personas de escasos recursos, personas con dificultades visuales o con bajísimo nivel educativo que hoy día no requieren mayor preparación para elegir una papeleta, ponerla en una urna y emitir su voluntad política, se verán enfrentados a un sistema mucho más complejo para votar.

Pero este no es el único inconveniente. Quizás el mayor problema es que aquellos que hoy auditan las elecciones en nuestro nombre (maestras de escuela, empleados públicos, fiscales de partidos políticos) se verán incapaces de auditar eficazmente un sistema de esta naturaleza. Solo personas altamente calificadas en ingeniería de software, electrónica y hardware podrán comprender el funcionamiento de estos sistemas. Incluso personal calificado en seguridad de sistemas de información se manifiesta incapaz de evaluar, validar y corroborar el funcionamiento correcto de urnas electrónicas. Estos mismos expertos difícilmente se atrevan a firmar a conciencia una certificación de seguridad de las urnas pues no existe método formal de validación que los avale.

Así, la participación real y tangible de la ciudadanía se verá reducida a la confianza ciega en un pequeño número de fiscales informáticos que, aun teniendo amplios conocimientos de la materia, no podrán certificar la validez de un resultado en el que todos los demás tendremos que confiar.

Si bien no existen sistemas perfectos, la diferencia de impacto es sustancial. Una mesa de votación tradicional puede registrar inconvenientes y ser anulada. El impacto sobre los resultados globales será mínimo. Sin embargo, un error mínimo en un sistema de votación electrónica puede alterar el resultado de una elección simultáneamente en un gran número de mesas.

6. Otros problemas generales

A todo esto vale agregar que, en la gran mayoría de los casos, los proveedores de urnas electrónicas son empresas privadas cuya composición accionaria deberíamos conocer en detalle antes de confiarles un proceso público y ciudadano como es la emisión del voto. ¿Cuáles serán los mecanismos para auditar a las empresas proveedoras? ¿Cómo sabremos cuáles son sus vinculaciones políticas y sus intereses en cada

elección? ¿Estamos dispuestos a privatizar un proceso ciudadano como el acto de votar?

Estas preguntas surgen a la luz de escándalos ocurridos en los EE. UU. donde, por ejemplo, uno de los principales accionistas de una de las empresas proveedoras de urnas (ES&S) resultó ser un senador republicano con obvios y marcados intereses en el resultado electoral.

FUENTES:

- https://blog.smaldone.com.ar/2017/03/26/que-es-el-voto-electronico/
- http://www.decoopchile.cl/voto-electronico-en-chile/

Capacitación en Comercio Electrónico y Gestión Web

"Tu futuro es creado por lo que haces hoy, no mañana."
Robert Kiyosaki

En la actualidad la tecnología avanza a pasos agigantados, incorporándose continuamente en todas nuestras actividades diarias, nuestras compras, consultas, pagos, transacciones, etc. Las realizamos en la comodidad de nuestros hogares, oficinas y/o lugares en los cuales se tenga acceso a Internet, a través de nuestros dispositivos móviles o computadores. Este avance ha permitido y obligado a que las grandes y pequeñas empresas, presenten sus productos y servicios a través del mismo medio, llegando a miles de usuarios en poco tiempo, mejorando sus ventas, así como, reduciendo los gastos en infraestructuras físicas y/o recursos en sus negocios.

Hoy en día las páginas web no se utilizan únicamente para informar, ahora son una vitrina al mundo, por lo que los negocios en línea requieren que sean administrados por personal experto, que realice una planificación y gestión adecuada y garantice el cumplimiento de objetivos y metas establecidas para su productividad.

SCProgress imparte cursos de capacitación en comercio electrónico, para que la creación y presentación de una tienda virtual grande o pequeña, cuente con las características indispensables para que sea rentable, así como, su gestión y seguimiento, mantengan a su negocio en el posicionamiento deseado.

Nuestra metodología se basa en el aprendizaje teórico – práctico, asegurando a los participantes una completa comprensión de las bases fundamentales de la creación y gestión de su negocio en línea.

El personal de capacitación es altamente especializado y goza de la experiencia necesaria para brindar la más completa información en los temas tratados en cada curso.

Esta vez, SCProgress pone a disposición de sus lectores y clientes, cursos de capacitación en los siguientes temas:

Curso de Comercio Electrónico	Curso de Gestión Web
Contenido: • Introducción al Comercio Electrónico • Modelos de negocio en Comercio Electrónico • Uso de embudos multicanal • Modelos de atribución • Seguimiento de eventos en Google Analytics • Analítica de publicidad y marketing en Internet • Redes sociales y Comercio Electrónico • El impacto de las redes sociales • Desarrollo de plan de negocios	**Contenido:** • Introducción a W3C • Principales comando de HTML5 • Diseño con HTML5 y CSS • Evaluación de sitios web • Diferentes tipos de portales web • Gestores de contenidos CMS • Caso práctico de CMS en Drupal • Uso de plantillas para la implementación de sitios web

• Evaluación de caso práctico	• Evaluación de rendimiento del sitio web • Seguimiento a través de SEO de Google Analytics

Los cursos se dictan en las instalaciones de SCProgress ubicadas en el edificio Plaza de Vizcaya, tercer piso, en La Pradera E7-21 y Mariana de Jesús,

Para mayor información visite nuestra página web: **www.scprogress.com**, o comuníquese directamente al correo electrónico: **ventas@scpgrogress.com**.

Ventajas y Desventajas del Voto Electrónico

El voto electrónico se ha impuesto en las contiendas electorales de la actualidad, y en este año en nuestro país va a existir una consulta popular en la cual los ciudadanos deben expresar su voluntad con su presencia en las urnas.

SCProgress considera oportuno presentar adicionalmente a los artículos expuestos, un breve resumen de las ventajas y desventajas del voto electrónico basándonos en el criterio de especialistas en voto electrónico de varias empresas muy reconocidas.

Ventajas:

- Los votos se contabilizan más rápido de lo normal y esto ahorra tiempo de muchas personas que tendrían que estar en las mesas electorales. Esta ventaja muy significativa.
- Para la persona que vota, le es mucho más fácil votar electrónicamente, es decir, por Internet, que votar con papeles.
- Como los votos son contabilizados por una computadora, se conocen los resultados de las elecciones al momento y esto es muy bueno ya que no hay ansias en la población del ganador. Esta es la mayor ventaja del voto electrónico.
- En parte, el Estado, tiene que invertir en la tecnología para poder lograr una correcta votación electrónica pero a la vez se ahorra la plata que tendría que pagar a las personas de las mesas electorales.
- La organización de las elecciones aumentaría debido a la implementación de las urnas electrónicas.
- Se necesitarán menos personas que trabajen durante la votación.
- El voto electrónico permite que no se suplante la identidad de otra persona, esto reduce en gran medida la probabilidad de que se alteren los resultados de las votaciones por suplantación de identidad.
- Otra de las ventajas del voto electrónico es que permite el rápido conteo de los votos por ende los entes gubernamentales encargados de dar los resultados de los sufragios electorales los pueden dar mucho más rápido, en algunos países la espere de tiempo se ha reducido casi en un 80% si se compara con el antiguo sistema de votación.
- En las elecciones electrónicas también se puede incluir como una ventaja es que al ser todo manejado electrónicamente ya los resultados no podrán ser alterados por situaciones tales como quema de votos, sustracción de votos o votos irregulares.

Desventajas:

- Como toda máquina o dispositivo tecnológico, puede fallar y a la vez puede haber un fraude electoral. Alemania, por ejemplo, no está de acuerdo con este tipo de votación porque sostiene la palabra de que no hay personas reales o con conocimientos suficientes para contabilizar los votos. Esta puede ser una desventaja significativa.

- Lamentablemente, como siempre, van a haber personas buscando vulnerabilidades en el sistema para poder modificar los datos de las elecciones. Es decir, que el sistema deberá poseer muchísima seguridad frente al público en general.
- El problema es que si hay fraude electoral debido a alguna persona que modificó los datos, nadie lo sabrá. Entonces, el pueblo tendrá a un gobernante que realmente no ganó, sino que lo impusieron.
- Tendrán que operar ingenieros altamente calificados para que no se infiltren datos de la votación, o para que no haya fallos. Es decir, que estas pocas personas sabias dentro del mundo informático, deberán estar pendientes de las elecciones en cuanto a cubrir cualquier fallo que pueda ocurrir en la tecnología.
- Otra posibilidad es que si se usa un software de una empresa privada se corre el riesgo de que dicho software haya sido diseñado para favorecer al gobierno que paga por el software.

Como pueden ver a pesar de ser un sistema avanzado, el voto electrónico no está a salvo de cualquier error o intervención de personas inescrupulosas.

FUENTES:

- http://gigatecno.blogspot.com/2013/12/ventajas-y-desventajas-del-voto.html
- http://www.miltrucosblogger.com/2014/02/ventajas-y-desventajas-del-voto-electronico.html

Seguridad en Cloud

SCProgress provee el servicio de seguridad en Cloud, basado en los estándares internacionales ISO, prevaleciendo y manteniendo su calidad mediante el uso permanente de los siguientes conceptos y normas:

Marcos de referencia y áreas de seguridad habituales.

ISO 27001
Norma que contiene las especificaciones de un sistema de gestión de la seguridad de la información (ISMS). Esta reemplaza a la antigua BS7799-2 standard.

ISO 27002
Estándar numérico de la serie 27000. Originalmente conocida como ISO 17799 standard. Antiguamente fue conocido como BS7799-1.

ISO20001

ISO 27003
Estándar oficial de un nuevo estándar con la intención de ofrecer una guía para la implementación de un ISMS.

ISO 27004
Estándar que cubre las especificaciones y métricas de un ISMS. Incluye como sugerencia los controles de la ISO 27002.

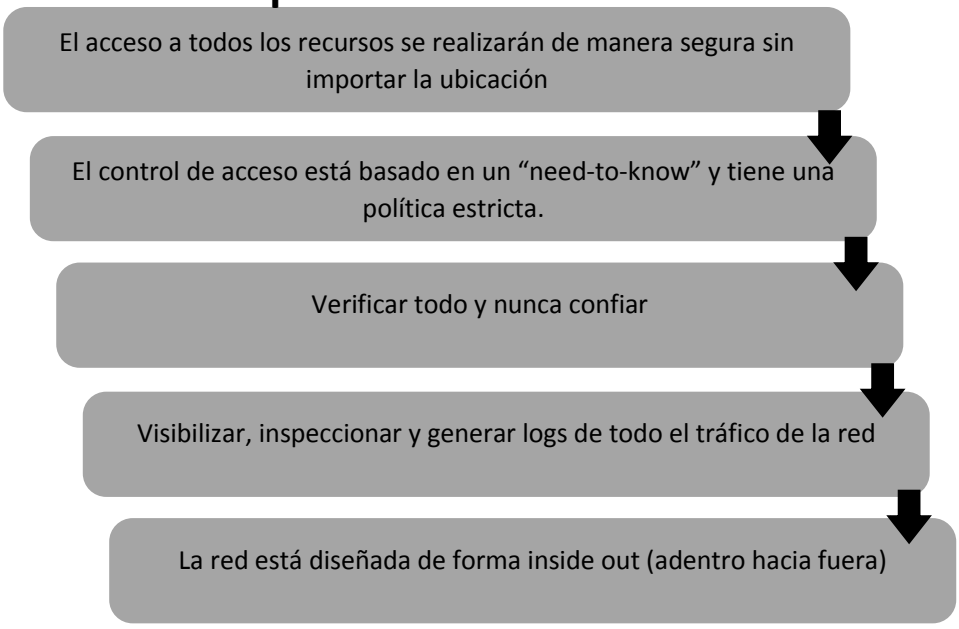
FedRAMP

ISO 27005
Metodología independiente de ISO para la administración de riesgo de la seguridad de la información.

ISO 27006
Estándar que provee guías para la acreditación de las organizaciones que ofrecen certificaciones ISMS.

Zero Trust

Conceptos del Zero Trust



¿ES REALMENTE POSIBLE HACKEAR UNA ELECCIÓN PRESIDENCIAL?

- “El único sistema seguro es aquél que está apagado en el interior de un bloque de hormigón protegido en una habitación sellada rodeada por guardias armados”, así de contundente se mostró Gene Spafford –experto en seguridad– cuando le preguntaron sobre la seguridad de los sistemas de voto.
- ¿Te imaginas que el presidente de tu país haya sido elegido por un hacker? Esta premisa, que parece sacada de una película de ciencia ficción, no está tan lejos como piensas. La posibilidad de que un especialista pueda intervenir los computadores de los candidatos, para robar información confidencial, hasta directamente hackear los sistemas de votación electrónica, no es remota.
- Por lo menos así quedó claro con la bullada entrevista del hacker colombiano Andrés Sepúlveda (31 años) en la revista Bloomberg, donde asegura haber intervenido varias elecciones dentro de Latinoamérica. En el texto titulado “Confesiones de un hacker político”, Sepúlveda asegura ser culpable de robar estrategias de campaña y bases de datos de diversos candidatos, como también de haber manipulado redes sociales e intervenido teléfonos personales.
- Estas acciones ilegales se habrían llevado a cabo, según Sepúlveda, en diferentes países de la región, entre ellos: Nicaragua, Panamá, Honduras, El Salvador, México, Costa Rica, Guatemala, Venezuela y Colombia.
- Dentro de este último país, el hacker colombiano cumple actualmente una condena de 10 años por los delitos de uso de software malicioso, conspiración para delinquir, violación de datos y espionaje, todos conectados al hackeo de las elecciones presidenciales de 2014.
- Sin embargo, muchos se preguntan si hackear una elección es realmente factible o en realidad sólo es posible en el mente de Sepúlveda. Si bien, varios involucrados han

intentado negar las acusaciones de este joven, Bloomberg asegura haber revisado y comprobado todas las confesiones del colombiano, incluso con expertos.

- “Este tiempo se caracteriza por los ataques dirigidos cuya naturaleza es atacar las víctimas seleccionadas cuidadosamente, bajo un interés específico, con el fin de espiar, extraer la información de la víctima y usarla para las ventajas del atacante. El ámbito político siempre ha sido un blanco de interés de esos ataques que han existido por lo menos desde hace unos 10 años.
- ¿Y el voto electrónico?
- Obviamente la posibilidad de intervenir campañas y bancadas políticas es sumamente importante. No obstante, qué pasaría si los hackers fueran más allá de lo que logró Sepúlveda e intentaran intervenir los sistemas de votación electrónicos. En la actualidad, dentro de Latinoamérica hay solamente tres países que han implementado esta tecnología. Brasil y Venezuela son los únicos que utilizan este sistema a nivel de sufragio, y que actualmente se encuentran estudiando servicios de biometría para asegurar las votaciones.
- El tercer país que cuenta parcialmente con esta tecnología es México. En este caso, al funcionar en un formato federal, el voto electrónico solamente ha sido aplicado en los estados de San Luis Potosí, Baja California, Coahuila, Distrito Federal, y Jalisco, aunque no a nivel nacional.
- Un caso similar ocurre en Argentina, donde este sistema ha sido implementado solamente en algunas partes del país, aunque nunca en elecciones nacionales de gran envergadura.
- A estos países se suman Bolivia, Chile, Ecuador, Paraguay, Panamá, Perú y Colombia, que cuentan con algunos casos experimentales en esta tecnología. En tanto, este último país es uno de los pocos que ya cuenta con una legislación para implementar esta plataforma electrónica.
- Pero, ¿qué pasa a nivel de seguridad? En la actualidad, solamente se han visto limitados casos de error con este sistema, principalmente en Estados Unidos y a nivel de funcionamiento técnico de las máquinas de votación. Un caso emblemático dentro de nuestra región ocurrió en Brasil, cuando en 2009 el investigador Sergio Freitas da Silva, uno de los 32 especialistas convocados por el Tribunal Superior Electoral de ese país para probar la seguridad de las urnas electrónicas, logró romper el secreto del sufragio con técnicas de lectura de radiofrecuencia y equipamiento muy económico. No obstante, el experimento sólo vulneró el secreto del voto y no la manipulación del conteo.
- “Cualquier plataforma y ambiente hoy día es posible de ser hackeado... El nivel de seguridad que tiene el voto electrónico debe ser integral para tener éxito, es decir, que la protección por capas, además de ser efectiva, tiene que ser 'inteligente'. Hablamos de inteligencia en el sentido de poder detectar una amenaza y proteger el ambiente de la forma más rápida posible para llevar al mínimo la posibilidad de que el ataque tenga éxito”.
- “Por lo general los sistemas de voto electrónico son sistemas de código propietario y por esto no es posible auditar el código. Pues éste no está disponible para el público, por lo menos por entero. Al tener esta circunstancia, no se puede de forma pública garantizar completamente que el código es libre de backdoors (accesos remotos no documentados), de bugs (agujeros de seguridad) y otros problemas. Claro está que los diseñadores de los sistemas de votos electrónicos se ciñen a los más altos estándares, pero nuevamente al no tener sus sistemas completamente “open source” o de código abierto, se dejan posibilidades de varios tipos de ataques”.
- Esta característica del voto electrónico lo transformaría en una plataforma especialmente vulnerable. Por otro lado, hasta

el momento tampoco existe un modelo formal (model checking) que garantice la seguridad de este sistema. Un paso básico para mostrar que no tiene fallas triviales.

- "El voto electrónico finalmente está basado en infraestructura física y virtual con aplicaciones que se comunican entre sí en tiempo real, y toda esta información debe ser almacenada en algún tipo de contenedor de datos; si nos damos cuenta, esto no es distinto del común de la infraestructura informática de cualquier empresa, pero con la diferencia de la connotación mucho más fuerte dado que está en "vitrina" de toda la ciudadanía y la comunidad internacional".
- La vulnerabilidad sin duda seguirá siendo un desafío para los países que ya cuentan con esta tecnología, y para los que evalúan sistemas biométricos para entregar más seguridad e identificar a los votantes. Porque una vulnerabilidad dentro de estas máquinas no significa simplemente que accedan a fotos comprometedoras o a mensajes privados en nuestros teléfonos, como ya estamos acostumbrados, sino que implanta directamente la posibilidad de poder hackear las democracias de la región.

FUENTES:

- https://tecno.americaeconomia.com/articulos/es-realmente-posible-hackear-una-eleccion-presidencial
- https://esnoticia.co/noticia-30009-voto-digital-voto-seguro

Rincón de los Expertos

.....

Asesoría y Consultoría en Comercio Electrónico

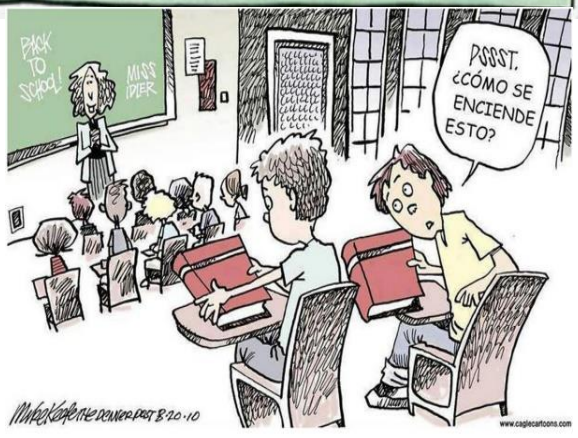
La gestión que marca la experiencia digital de sus compradores, requiere del asesoramiento para mejorar las prácticas de trabajo en su negocio digital, a través de profesionales altamente especializados en temas tan imprescindibles como:

- **Innovación & Design Thinking**
- **Procesos creativos para la creación de productos y servicios de valor**
- **Análisis de Mercados, descubrimiento de necesidades y propuestas de valor**
- **Estrategias de manejo efectivo de clientes**
- **Técnicas de Negociación y Manejo de Reuniones**
- **Emprendimiento tecnológico**
- **Márketing para Pymes de IT**
- **Finanzas del emprendedor**
- **El modelo Canvas y la Planificación estratégica**
- **El modelo Canvas y la Marca Personal**
- **Cultura Corporativa enfocada en los negocios y las personas**
- **Lectura Política, Económica y Social del entorno de negocios**
- **Networking y Asociación Social de negocios para Ejecutivos de IT**

La gestión y administración de su empresa online, en conjunto con el seguimiento adecuado de clientes, pueden mejorar, desarrollar y establecer prácticas y procesos para atraer, retener e incrementar su base de datos de nuevos clientes.

La era digital y los negocios en línea se encuentran en progreso y desarrollo continuo. Contáctenos en el correo electrónico: **camiranda33@hotmail.com**, un asesor le brindará la información necesaria, de acuerdo a sus requerimientos y los de su empresa.

Humor



Noticias

E-commerce: Consumidores Perciben los Productos más Baratos, Incluso Cuando su Precio es Mayor

La principal ventaja del e-commerce es la comodidad del usuario. ¿Quieres implementarlo en tu compañía? No te pierdas el vídeo con los tres mejores consejos de Nielsen para lograrlo.

Shoppers, buyers y consumidores, la santísima trinidad del marketing que hace eco en los pasillos corporativos del mundo en busca de responder una sola pregunta: ¿cómo vender más y mejor? La palabra clave es innovar. Así lo entiende Carlos Altieri, VP de soluciones estratégicas de Nielsen para mercados emergentes de Latinoamérica. En primer lugar, debemos diferenciar al shopper del consumidor del buyer, señaló a Gestion.pe Altieri.

“El shopper no es un buyer. Un buyer es alguien que estuvo en la tienda, cogió algo y lo compró. El shopper somos todos los que vamos a una tienda y podríamos haber hecho una transacción”, señaló. Esta primera diferencia puede ser crucial para nuestros objetivos de marketing. “No es lo mismo cómo una promo le habla a un consumidor que a alguien que solo está dentro de la tienda”, añadió. Incluso, una promoción mal ubicada o dirigida al público equivocado puede ser fácilmente percibida como contaminación visual.

De hecho, el 46% de latinoamericanos siente como una “obligación” el ir de compras, y prefiere dedicarle el menor tiempo posible, según Nielsen.

Si a eso le sumamos una publicidad mal segmentada, el efecto puede ser nocivo. E-Commerce Digital es el futuro. Sin embargo, para entender cómo vender en digital, solo hace falta entender cómo vender en sí. “El driver básico de por qué uno va a comprar es la conveniencia: ‘me quedó la tienda de paso, estaba cerca, tenía que comprar algo y llegué a otro local’”, subrayó Altieri. En la Internet ocurre exactamente lo

mismo, solo que reconfigurado con la camiseta e-commerce. La información que manejan las tiendas, con sus enormes bases de datos, descubren una segmentación mucho más precisa y personal para entender quién es nuestro shopper, buyer y consumidor. Un programa de loyalty o lealtad bien empleado puede generar data interesante sobre el ticket promedio de nuestros clientes y qué compran. “Nos permite hasta pensar mejor las promociones porque ya te conozco y sé qué te puede interesar y en donde colocar los descuentos”, apuntó el experto.

Es decir, trasladar la experiencia de la tienda física al espacio virtual, pero con una ventaja considerable: el 89% de latinos percibe los precios online como iguales o menores que en las tiendas físicas. Incluso cuando el precio web es más caro, sigue siendo percibida como un ahorro para el humano corriente. Y es que el valor de no levantarse de la cama, coger las zapatillas y hacer la cola mientras oye la vigésimoquinta versión de la canción de moda es invaluable para el cliente.

Este mismo insight se encuentra detrás del reciente éxito de los canales de proximidad. Estas cadenas de tiendas pequeñas diseminadas por la ciudad y que ofrecen desde empanadas hasta cervezas, crecen en 36% en la región. Y para que vean la importancia de la locación, para el 56% de latinoamericanos este sencillo aspecto es determinante en el proceso de compra. “Las grandes superficies no crecen, sino el convenience. El crecimiento viene por el lado de superficies más chicas, como una cadena de bodegas súper sofisticada”, anotó.

FUENTE:

https://gestion.pe/empleo-management/commerce-consumidores-perciben-productos-mas-baratos-incluso-cuando-su-precio-mayor-2200491

SCProgress cuenta con todo lo que necesita para su infraestructura de cableado estructurado

Los sistemas de cableado estructurado constituyen una plataforma universal para la transmisión de voz, datos y video, el diseño e implementación de infraestructuras de fibra óptica y cableados que cumplan con los estándares se vuelven cada vez más imprescindible para el éxito de sus empresas.

SCProgress brinda el mejor servicio en:

- Diseño e instalación de sistemas de cableado estructurado con las mejores marcas.
- Certificación de sistemas de cableado estructurado
- Diseño e instalación de fibra óptica.
- Asesoría técnica para la implementación de sistemas de cableado estructurado.
- Personal altamente calificado, certificado y con amplia experiencia.

En caso de requerimiento del cliente, nuestro personal cuenta con experiencia en marcas como Panduit, Dexon, así como marcas nacionales.

Para más información no dude en contactarnos en ventas@scprogress.com

GESRICA
COMPAÑÍA DE GESTIÓN DE RIESGO Y CAPACITACIÓN S.A.

Nuestro país se encuentra ubicado sobre el cinturón de fuego del pacífico, por lo que nos encontramos expuestos a eventos naturales que pueden afectar nuestras actividades, razón por la cual, debemos tomar acciones y ejecutar procedimientos para mitigar posibles siniestros, ya sean causados por la fuerza de la naturaleza o por accidentes humanos.

Contamos con personal especializado en la gestión, planificación, capacitación e implementación de estrategias para la reducción de riesgos y ponemos a su disposición , asesoramiento en la elaboración de planes de gestión de riesgos, diseñados exclusivamente para las características de su empresa, así como, capacitación en áreas a fines, principalmente en:

- ***Primeros auxilios.***
- ***Brigadas de emergencia.***
- ***Prevención de incendios***
- ***Seguridad industrial.***
- ***Normas de seguridad.***
- ***Prevención y manejo de emergencias y evacuaciones.***

www.gesrica.com
E-mail: info@gesrica.com
Teléfonos: 0984489267 - 0996620889 – 0979003123
Dirección: 18 de Septiembre 07-04-009 y Panamericana Norte.

www.scprogress.com

Octubre 2017