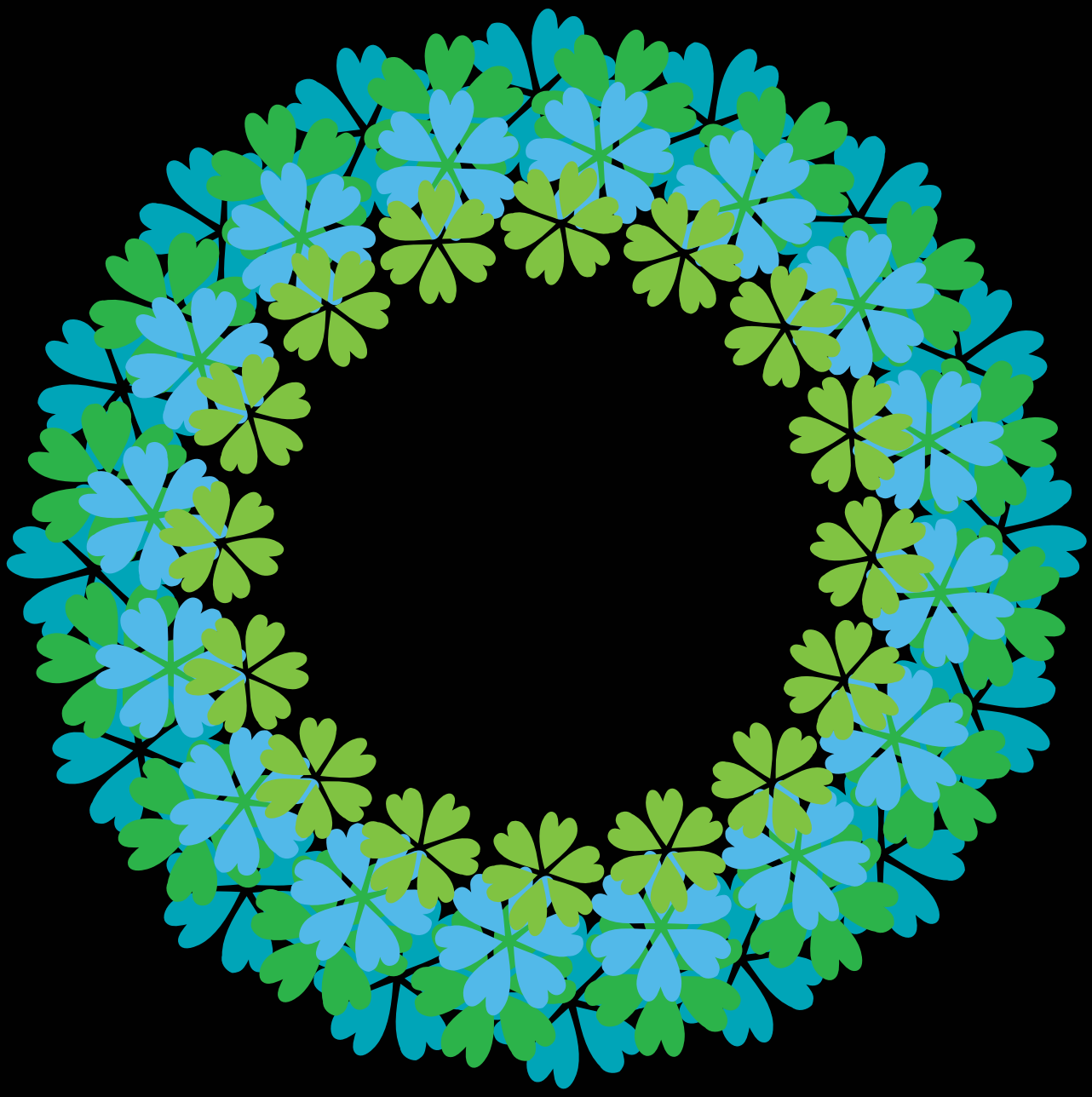
Informativo *Gerencial*

Junio | 2017

Generamos impactos que trascienden



50 años

Deloitte.
Ecuador

Contenido



03

¿Qué aporta a la alta dirección un reporting de ciberseguridad?
What is the role of senior management in cybersecurity reporting?

08

Convenios para evitar la doble tributación
Agreements to avoid double taxation

10

Registros Oficiales
Official Register

12

Cifras Económicas
Economic Indicators

¿Qué aporta a la alta dirección un reporting de ciberseguridad?

Por: Ricardo Martínez Martínez, socio de Governance, Risk & Compliance, Deloitte España

¿La dirección de las compañías es realmente consciente de los riesgos y reflexiona sobre las ciberamenazas? ¿Son conocedores de la estrategia, planes y medios que tienen para defenderse de un ciberataque?

Cada minuto que transcurre en los negocios y empresas, los ciberatacantes son más numerosos y mucho más sofisticados. Esto hace que el número de ciberataques aumente significativamente y, con ello, que cada ataque se muestre más devastador para las organizaciones y los negocios que generan. En este sentido, y aunque pueda no parecer así, es ahora cuando las compañías se están empezando a dar cuenta de que no es tanto una cuestión de "SI" ellos serán atacados, sino de "CUÁNDO" sufrirán el ataque.

A pesar de que estén empezando a despertar y pensar que es cuestión de tiempo, todavía existen grandes organizaciones que están ignorando lo que puede haber detrás de una amenaza de ciberseguridad. Muchas se dan cuenta sólo cuando ocurre algún incidente que les afecte. Y si es grave, es cuando los accionistas y gestores empiezan a pedir explicaciones y responsabilidades. Hoy en día, y según diferentes estudios y la experiencia

Every minute spent in business and businesses, cyberattacks are more numerous and much more sophisticated. This means that the number of cyber-attacks increases significantly and, with it, that each attack is more devastating for the organizations and businesses that generate. In this sense, and although it may not seem like this, it is now when companies are beginning to realize that it is not so much a matter of "IF" they will be attacked, but of "WHEN" they will undergo the attack.

Although they are beginning to wake up and think that it is a matter of time, there are still large organizations that are ignoring what may be behind a cybersecurity threat. Many realize it only when something happens that affects them. And if it is serious, it is when the shareholders and managers begin to ask for explanations and responsibilities. To act out. Nowadays, and according to different studies and own experience, only a handful

Are they aware of the strategy, plans and means they have to defend themselves against a cyber-attack?

Hay que recordar que los ciberataques, pretenden obtener en primer lugar una buena dosis de información, de forma ilegal en la mayoría de las ocasiones, de las organizaciones y sus directivos, para continuar provocando otra serie de situaciones de riesgo.

propia, tan solo un puñado de empresas tienen implantadas unas ciberdefensas maduras y a la altura como para responder con éxito a un ciberataque contundente y persistente.

Entre otras: un quebranto económico directo, beneficiándose los atacantes del mismo; un daño reputacional y/o deterioro de la marca, provocando una pérdida de la confianza de los clientes; un obstáculo en las operaciones de sus negocios; e incluso la destrucción de las infraestructuras críticas de una nación. Todo ello, sin olvidarse, claro, del posible incumplimiento regulatorio, con sanciones incluidas, que la vulneración de un sistema de control en las organizaciones puede provocar sobre las mismas, sus accionistas / directivos.

Y con todo ello, ¿la Dirección de las compañías es realmente consciente de los riesgos y reflexiona de verdad sobre este asunto? ¿Son conocedores de la estrategia, planes y medios que tienen para defenderse de un ciberataque? ¿Saben si están focalizados en los aspectos más críticos? ¿Cubren esas medidas la responsabilidad del Consejo y su Dirección? ¿Entienden los ejecutivos el impacto potencial de un ciberataque? ¿Están preparados para responder a clientes, reguladores y otras partes sobre la gestión del ciberriesgo? Y, por último, entre otras cuestiones, ¿están en disposición de responder a tiempo y con solvencia a un ciberataque? El tiempo de reacción es un factor clave.

Según un estudio de Deloitte, el "EMEA 360º. Boardroom Survey", que trata las principales preocupaciones en las agendas de los consejeros, la ciberseguridad se encuentra en la posición 13 como preocupación de los diretivos para los próximos 12 y 24 meses. Por delante de otras como puedan ser la gestión de sucesiones, estructura organizativa, crisis financiera mundial y recuperación, gobierno, refinanciación o riesgo fiscal.

El surgimiento de la ciberseguridad como un problema significativo puede deberse, además de lo mencionado anteriormente, a su visibilidad en los informes de medios de comunicación y a la creciente amenaza de riesgos para la reputación de las empresas. El riesgo en materia de ciberseguridad no es la exposición a un solo suceso para el que se pueda aplicar una solución específica en un momento determinado, sino que evoluciona, y las medidas de seguridad exigen revisiones y actualizaciones periódicas en toda la empresa. El problema va mucho más allá del departamento informático; el Consejo de Administración es uno de los responsables

of companies have established cyberdefen-sas ripe and at the height to successfully respond to a strong and persistent cyber-at-tack.

It should be remembered that these attacks, the cyber-attacks, are intended to obtain, in the first instance, a good amount of information, in an illegal way in most cases, of the organizations and their managers, to continue provoking another series of risk situations.

Among others: a direct economic loss, benefiting the attackers of the same, A reputational damage and / or deterioration of the brand, causing a loss of the trust of the customers; an obstacle in the operations of their businesses; And even the destruction of a nation's critical infrastructures. All this, without forgetting, of course, the possible regulatory breach, with sanctions included, that the violation of a control system in organizations can provoke on them and their shareholders / managers.

And with all this, is the company management really aware of the risks and really reflects on this matter? Are they aware of the strategy, plans and means they have to defend themselves against a cyber-attack? Do you know if they are focused on the most critical aspects? Do these measures cover the responsibility of the Board and its Board? Do executives understand the potential impact of cyberattacks? Are they prepared to respond to customers, regulators and other parties about cyber risk management? And, finally, among other issues, are they willing to respond in time and with credit to a cyber-attack? Reaction time is a key factor.

According to a Deloitte study, the "EMEA 360º. Boardroom Survey ", which addresses the main concerns in the Counselors' agendas, Cybersecurity is in position 13 as a concern of the same for Directors for the next 12 and 24 months. Ahead of others such as succession management, organizational structure, global financial crisis and recovery, government, refinancing or fiscal risk.

The emergence of cybersecurity as a significant problem may be due, in addition to the above, to its visibility in media reports and the growing threat of risk to corporate reputation. The risk in cybersecurity is not exposure to a single event for which a specific solution can be applied at any given time, but evolves, and security measures require periodic updates and updates throughout the enterprise.

en última instancia.

Por ello, es imprescindible que éste último reciba un adecuado reporte de la valoración periódica de su organización en términos del nivel de protección, los mecanismos de vigilancia de que dispone y, sobre todo, la preparación que tienen para dar respuesta y recuperar la normalidad en caso de un ciberataque.

Por tanto, el cuadro de mando que les tendría que llegar debería proporcionarles una visibilidad sobre el estado general de la ciberseguridad en relación con los objetivos de negocio, de forma que permita un mejor control de la ciberseguridad. Asimismo, es esencial que tenga foco en lo importante para el negocio, entendiendo qué indicadores tienen un impacto más tangible para su actividad y objetivos estratégicos.

Dichos reportes deben contemplar los siguientes factores:

Entendible
Los indicadores clave deben ser entendidos por cualquiera que tenga acceso a ellos. Lo que es obvio e intuitivo para un profesional de la seguridad puede no serlo para un ejecutivo de negocio.

Conciso
El reporting de ciberseguridad debe ser un informe más sobre la mesa de la Alta Dirección. El tiempo disponible es limitado, por lo que es importante priorizar la calidad con respecto a la cantidad.

Comparable
Idealmente, un indicador debe poder ser comparado. Por ejemplo, a través de diferentes periodos de tiempo, para mostrar evolución o identificar tendencias.

Parecen evidentes, pero muchas organizaciones no disponen de un reporting de ciberseguridad similar, cuidando estas cualidades y consiguiendo un óptimo grado de utilidad gracias a la selección adecuada de sus indicadores. Hay que seguir trabajando en las organizaciones en lograr un marco de información útil, práctico y efectivo, sin olvidar que todavía se requiere mucha concientización y formación en todos los posibles stakeholders: desde los empleados y directivos, hasta clientes y proveedores relacionados. A todos ellos se les debería implicar de una u otra manera en las actividades y estrategias de ciberseguridad de la organización.

El alcanzar o no unos niveles de madurez razonables en la gestión de la ciberseguridad

Cada vez es más evidente que la Alta Dirección requiera de información del grado de exposición que tienen sus organizaciones al ciberriesgo, como un riesgo más a contemplar en sus valoraciones.

The problem goes far beyond the IT department; the Board of Directors is ultimately responsible.

Therefore, it is imperative that the latter receive an adequate report of the periodical assessment of their organization in terms of the level of protection, the monitoring mechanisms available to them and, above all, the preparation they have to respond and recover normality in Case of a cyber-attack.

It is increasingly evident that top management and councils require information on the degree of exposure that their organizations have to cyber risk, as one more risk to contemplate in their assessments. Therefore, the scorecard that should reach them should provide them with visibility into the overall state of cybersecurity in relation to business objectives, so as to allow better control of cybersecurity. It is also essential that you focus on what is important to the business, understanding which indicators have a more tangible impact on your business and strategic objectives.

Those scorecards should be:

Understandable
Key indicators should be understood by anyone who has access to them. What is obvious and intuitive for a security professional may not be for a business executive.

Concise
Cybersecurity reporting should be a further report on the Board. The time available is limited, so it is important to prioritize quality with respect to quantity.

Comparable
Ideally, an indicator should be able to be compared. For example, across different time periods, to show evolution or identify trends.

They seem obvious, but many organizations do not have a similar cybersecurity reporting, taking care of these qualities and obtaining an optimal degree of utility thanks to the adequate selection of their indicators. We must continue to work in organizations to achieve a useful, effective and effective information framework, not forgetting that a lot of awareness and training is still required in all possible stakeholders: from employees and managers, to clients and related suppliers. All of them should be involved in one way or another in the activities and cybersecurity strategies of the organization.

solo será posible si se extreman las medidas y se establecen todos los controles posibles para mitigar los riesgos de este tipo en las organizaciones. En este sentido es fundamental la inclusión de los ciberriesgos en la función de gestión de riesgos de las compañías, y otorgar la valoración a los mismos conforme a la objetividad de las variables de medición del modelo que se esté utilizando.

Para poder conseguir ese nivel de respuesta, una aproximación que están llevando a cabo algunas organizaciones es integrar la ciberseguridad en los modelos que ya disponen de las tres líneas de defensa, donde cada una de ellas juega un papel relevante en la protección y mejora del marco de control necesario y establecido.

Desde la primera, donde los controles deben de estar en todos los procesos con un riesgo ciber posible e identificado por las distintas áreas de negocio. Pasando por la segunda a través de las funciones de gestión de riesgos, compliance, asesoría jurídica, etc... Y llegando a esa auditoría interna que representa la tercera línea. Evidentemente, esta presencia requiere de mucha sensibilización en las organizaciones, pero más aún, de personal convenientemente formado y capaz de cubrir estos gaps, que, aunque son técnicos en su base, necesitan de una importante comprensión del impacto que tienen en los objetivos del negocio.

El crecimiento de los ciberataques, son exponenciales, y el impacto de los mismos son devastadores. Detrás de los atacantes hay muchos intereses, y ya no solo personales, sino también políticos, sociales, de competencia, estratégicos...

Los escándalos y ejemplos de ciberataques que se suceden cada día en las compañías, y en la sociedad en general, han hecho que llegue al interés de los altos estamentos de las organizaciones. El peso que le han dado los reguladores a la responsabilidad de los gestores también influye notablemente en esta preocupación. **Es por ello que hay que aprovechar la oportunidad e informar con claridad y simplicidad en primer lugar, y con miras a hacerlo holísticamente e integrado con otros reportes que ya hoy en día les llegan.**

Reaching reasonable levels of maturity in cybersecurity management will only be possible if action is taken and all possible controls to mitigate such risks in organizations are established. In this sense, it is fundamental to include cyber risk in the risk management function of the companies, and to give the valuation to them according to the objectivity of the measurement variables of the model being used.

In order to achieve this level of response, an approach being undertaken by some organizations is to integrate cybersecurity into models that already have the three lines of defense, each of which plays a relevant role in the protection and improvement of the framework of necessary and established control.

From the first, where the controls must be in all processes with a possible cyber risk and identified by the different business areas. Going through the second through the functions of risk management, compliance, legal advice, etc ... And reaching that Internal audit that represents the third line. Obviously, this presence requires a great deal of awareness in organizations, but even more, of adequately trained personnel capable of covering these gaps, which, although they are technicians at their base, need an important understanding of the impact they have on business objectives.

In addition, these cybersecurity reports should include the necessary measures to be put in place, grouped into action plans to help mitigate identified cyber risks. Without this, and a follow-up of such incidents, the report would be incomplete.

The growth of cyber-attacks, are exponential, and their impact is devastating. Behind the attackers there are many interests, and not only personal, but also political, social, competitive, strategic.

The scandals and examples of cyberattacks occurring every day in companies, and in society in general, have made it come to the interest of the high levels of organizations. The weight that regulators have given to the responsibility of managers also has a significant influence on this concern. **That is why we must seize the opportunity and inform with clarity and simplicity in the first place, and with a view to making it holisti-cally and integrated with other reports that already reach them today.**

Asimismo, estos informes de ciberseguridad deberían contemplar las medidas necesarias poner en marcha, agrupadas en planes de acción que ayuden a mitigar los ciberriesgos identificados. Sin esto, y un seguimiento de dichas incidencias, el reporte quedaría incompleto.

Deloitte.

PECB

ISO 27001 - Seguridad de la Información
Certificación Auditor Líder

12 al 16 de junio, 2017 - Hotel Swissotel, Quito

Costo del curso ISO 27001: $1,650

Los cursos serán dictados por **instructores certificados** por el PECB e incluyen **examen de certificación avalado** por el mismo organismo y reconocido internacionalmente.

Recibe:

5% de descuento si se inscriben 2 o 3 personas*.

10% de descuento si se inscriben 4 o más personas*.

Si se cancela antes del inicio del curso tiene un ***5%*** de descuento adicional.

* Válido para personas de la misma organización.

Convenios para evitar la doble tributación

Por: Juan Yupa, Director Tax, Deloitte Ecuador

De acuerdo a la Constitución del Ecuador, la aplicación de los tratados y convenios internacionales, está sobre las leyes y demás normativa ecuatoriana.

Desde 1986 Ecuador ha suscrito convenios para evitar la doble tributación en materia de impuesto a la renta y sobre el Patrimonio con diferentes países, los cuales tienen como objetivo, establecer el tratamiento tributario que aplica a las transacciones que se generan entre 2 países, a fin de evitar que las mismas tributen 2 veces.

Una de las facultades del Servicio de Rentas Internas – SRI es efectuar la determinación recaudación y control de los tributos internos del Estado. Al respecto se han emitido varias disposiciones tributarias que le permiten controlar la aplicación de los convenios para evitar la doble tributación, a continuación un recuento de dichas disposiciones hasta llegar al procedimiento aplicable para el año 2016.

Entre 1986 y hasta el año 2001, podemos señalar que se aplicaban los convenios de forma automática, sin la presentación o el cumplimiento de algún requisito o procedimiento adicional.

A partir del año 2002 se estableció como requisito para soportar la aplicación automática de los convenios para evitar la doble tributación, la obligatoriedad de obtener un certificado de residencia fiscal del proveedor, emitido por la autoridad tributaria del país con el cual Ecuador suscribió el Convenio. Este certificado debía ser traducido al castellano, consularizado y actualizado cada 6 meses.

As of 1986, Ecuador has signed various agreements with different countries to avoid levying income tax and tax on capital twice. Such agreements are designed to establish the tax treatment applicable to transactions generated between 2 countries and avoid the same tax being applied twice.

One of the faculties of the Internal Revenue Service (SRI) is to oversee the collection and control of internal State taxes. A summary of the various tax provisions providing for control of agreements to avoid double taxation up to the present date is set out below.

Between 1986 and 2001, application of agreements was automatic, without the need for any additional requirement or procedure.

As of 2002, a certificate of the provider's tax residence, issued by the tax authority of the country with which Ecuador had signed the respective agreement, was required for the automatic application of agreements to avoid double taxation. A translation of the certificate into Spanish was also required, legalized through the Ecuadorian consulate nearest to the place of issue and updated every 6 months.

Under the Ecuadorian Constitution, application of international treaties and agreements prevails over Ecuadorian law and other regulations.

Luego de 6 años, a partir del año 2008 se estableció un nuevo requisito, los gastos deberían encontrarse certificados por auditores independientes que tengan sucursales, filiales o representación en Ecuador, la certificación se debe referir a la pertinencia del gasto para el desarrollo de la actividad de la compañía ecuatoriana.

El certificado debía ser emitido por el auditor independiente en el país donde se encontraba domiciliado el proveedor, país con el cual Ecuador suscribió el Convenio. A finales del año 2008, se permitió que el certificado sea emitido una parte en el exterior y otra parte en Ecuador.

El control del SRI se efectuaba con posterioridad a la aplicación de los convenios, solicitando los certificados, a los auditores externos de las compañías, a través del informe de cumplimiento de obligaciones tributarias; o, en los procesos de determinación solicitando directamente a las Compañías.

Durante el año 2016 se han efectuado ciertas reformas, con las cuales el control por parte del SRI, a la aplicación de los Convenios, es más directo; el nuevo procedimiento establecido se detalla a continuación:

- Se establece como valor máximo, para aplicar automáticamente los beneficios previstos en los convenios, 20 fracciones básicas gravadas con tarifa 0% de impuesto a la renta para personas naturales, es decir, para el año 2016 hasta US$223,400. Este máximo aplica por proveedor y por ejercicio económico.

- Si el valor facturado por el proveedor supera el valor mencionado, sobre el exceso se debe efectuar la retención en la fuente de impuesto a la renta, aplicando el porcentaje general en pagos al exterior (22%),a pesar de que el Convenio no establece este procedimiento.

- Posteriormente, el proveedor extranjero podrá solicitar al SRI la devolución de la retención en la fuente, que en base al Convenio no se debió efectuar. Es en este momento que el SRI efectuaría el control directo sobre la aplicación de los Convenios.

6 years later, as from 2008, a new requirement was imposed, requiring expenses to be certified by independent auditors with branches, affiliates or representation in Ecuador. The certificate had to reference the relevance of the expense with respect to development of the activities of the Ecuadorian company.

The certificate also had to be issued by an independent auditor in the country in which the provider was domiciled and with which Ecuador had signed an agreement. A further requirement was added at the end of 2008, one part of the certificate to be issued abroad and the other part in Ecuador.

Control imposed by the SRI was subsequent to the application of the agreements. Companies' external auditors were required to provide certificates through tax compliance reports or in assessments process in which such information was requested directly from the companies.

Year 2016 saw various reforms implemented by the SRI and through which control of the application of agreements has become more direct, as described below.

- Automatic application of benefits provided by the agreements is now subject to a limit of 20 times the tax free allowance for an individual (US$223,400 for year 2016). This maximum is applicable to each provider for each fiscal year.

- Any excess invoiced by the provider is subject to income tax withholdings at source at the tariff applicable to payments remitted overseas (22%), irrespective of the agreements not mentioning such limitations.

- The overseas provider may, subsequently, request a refund of the withholding at source from the Internal Revenue Service (SRI) which, under the agreement, should not have been performed. Through such mechanism the SRI now exercises control of the application of agreements to avoid double taxation.

Registros oficiales

Área Político Administrativa

(R.O. No. 1004; 15-05-2017)
Resolución No. RESCGEN-DMT-2017-00002 del Municipio del Distrito Metropolitano de Quito. Se amplía el plazo para la presentación de la declaración del Impuesto de patente para personas naturales no obligadas a llevar contabilidad, correspondiente al ejercicio fiscal 2016.

(S-R.O. No. 1005; 16-05-2017)
Decreto Ejecutivo No. 1372. Se reforma el reglamento General de Aplicación de la Ley Orgánica de Incentivos para Asociaciones Público-Privadas y la Inversión Extranjera.

(S-R.O. No. 1; 25-05-2017)
Decreto Ejecutivo No. 1417. Se reforma el Reglamento General del Código Orgánico de Planificación y Finanzas Públicas.

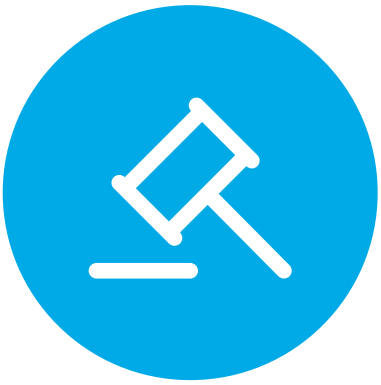
Área Tributaria

(S-R.O. No. 990; 24-04-2017)
Resolución No. NAC-DGERCGC17-00000260 del Servicio de Rentas Internas. Se establecen las normas generales para la retención en la fuente del impuesto a la renta a cargo del propio sujeto pasivo en la comercialización y/o exportación de productos forestales.

(S-R.O. No. 999; 8-05-2017)
Resolución No. NAC-DGERCGC17-00000273 del Servicio Rentas Internas. Se amplía el plazo para la presentación de la Declaración Patrimonial correspondiente al año 2017.

Área Financiera

(R.O. No. 997; 4-05-2017)
Resolución No. SB-2017-279 de la Superintendencia de Bancos. Se expide la Norma de control para las juntas generales de accionistas de las entidades bajo el control de esta Superintendencia.



Administrative Policy Area

(R.O. No. 1004; 15-05-2017)
Resolution No. RESCGEN-DMT-2017-00002 of the Municipality of the Metropolitan District of Quito extends the period for filing the License Tax ("Impuesto de Patente") for individuals not required to maintain accounting records with respect to year 2016.

(S-R.O. No. 1005; 16-05-2017)
Executive Decree No. 1372 amends the General Application of the Incentives for Public-Private Partnerships and Foreign Investment Law.

(S-R.O. No. 1; 25-05-2017)
Executive Decree No. 1417 amends the General Application of the Public Planning and Financing Code.

Tax Area

(S-R.O. No. 990; 24-04-2017)
Resolution No. NAC-DGERCGC17-00000260 of the Internal Revenue Services establishes general regulations for income tax withholdings at source payable by taxpayers undertaking the sale and/or export of forestry products.

(S-R.O. No. 999; 8-05-2017)
Resolution No. NAC-DGERCGC17-00000273 of the Internal Revenue Services extends the period for filing the Equity Return for year 2017.

Finance Area

(R.O. No. 997; 4-05-2017)
Resolution No. SB-2017-279 of the Superintendence of Banks issue the control Regulation with respect to General Shareholders' Meeting of entities under the control of this Superintendence.

(R.O. No. 1001; 10-05-2017)
Resolución No. 350-2017-F de la Junta de Política y Regulación Monetaria y Financiera. Se reforma la Resolución No. 249- 2016-F "Política para la desinversión de acciones de propiedad de entidades del sector financiero público"

(R.O. No. 1010; 23-05-2017)
Resolución No. 335-2017-F de la Junta de Política y Regulación Monetaria y Financiera. Se expide la Norma para la autorización y funcionamiento en el país de sucursales y oficinas de representación de entidades financieras extranjeras.

Resolución No. SB-2017-319 de la Superintendencia de Bancos. Se reforma el capítulo I "Normas para la contratación de las auditoras externas que ejerzan su actividad en las entidades sujetas al control de la Superintendencia de Bancos y Seguros"; Título XXI, Libro I de la Codificación de Resoluciones de la Superintendencia de Bancos; y otros.

(R.O. No. 1001; 10-05-2017)
Resolución No. SB-2017 – 296 de la Superintendencia de Bancos. Se expide la Norma para la Aplicación de las Disposiciones Transitorias Cuadragésima Tercera, Cuadragésima Cuarta y Cuadragésima Quinta del Código Orgánico Monetario y Financiero.

Área Procesal

(S-R.O. No. 1003; 12-05-2017)
Resolución No. 047-2017 del Consejo de la Judicatura. Se aprueban los formularios únicos: para petición de divorcio por mutuo consentimiento; para petición de terminación de la unión de hecho por mutuo acuerdo; de solicitud de nuevo día y hora para audiencia de conciliación en el trámite de divorcio por mutuo consentimiento; y, de solicitud de nuevo día y hora para audiencia de conciliación en el trámite de terminación de la unión de hecho por mutuo acuerdo.

Área de Turismo, Medio Ambiente, Transporte, Comunicaciones, Electrificación, Petróleo, Salud.

(S-R.O. No. 998; 5-05-2017)

Función Legislativa. Se expide la "Ley Orgánica del Sistema Nacional de Infraestructura vial del Transporte Terrestre".

(R.O. No. 1001; 10-05-2017)
Resolution No. 350-2017-F of the Monetary and Finance Policy and Regulatory Board amends Resolution No. 249- 2016-F "Policy for divesting shares owned by public finance sector entities"

(R.O. No. 1010; 23-05-2017)
Resolution No. 335-2017-F of the Monetary and Finance Policy and Regulatory Board issues the Regulation for the authorization and operation of representation branches and offices of foreign financial entities in Ecuador.

Resolution No. SB-2017-319 of the Superintendence of Banks amends chapter I "Standards governing the hiring of external auditors undertaking activities in entities under the control of the Superintendence of Banks and Insurance"; Title XXI, Book I of the Codification of Resolutions of the Superintendence of Banks and others.

(R.O. No. 1001; 10-05-2017)
Resolution No. SB-2017 – 296 of the Superintendence of Banks issues the Regulation for Application of the Forty-Third, Forty-Fourth and Forty-Fifth Temporary Provisions of the Monetary and Finance Code.

Procedural Area

(S-R.O. No. 1003; 12-05-2017)
Resolution No. 047-2017 of the Judicial Council approves the single forms for petitioning for divorce by mutual consent; for petitioning the termination of a common law relationship by mutual consent; for requesting a new date and time for a reconciliation hearing for divorce through mutual consent; and for requesting a new date and time for terminating a common law relationship by mutual consent.

Tourism, Environmental, Transport, Communications, Electrification, Oil and Health Area

(S-R.O. No. 998; 5-05-2017)

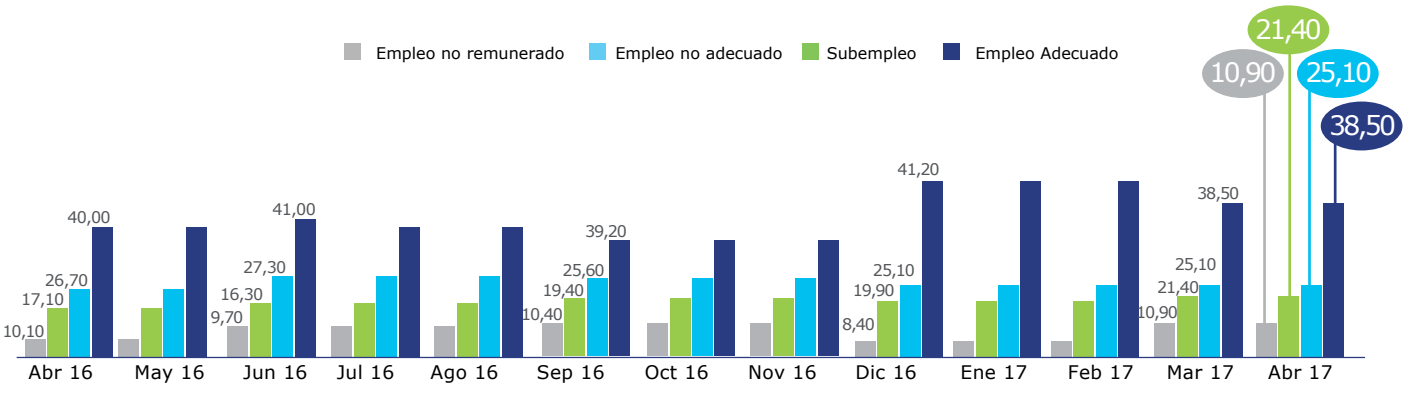
The Legislative Function issues the "Law for the National Land Transport Highway Infrastructure"

Cifras económicas

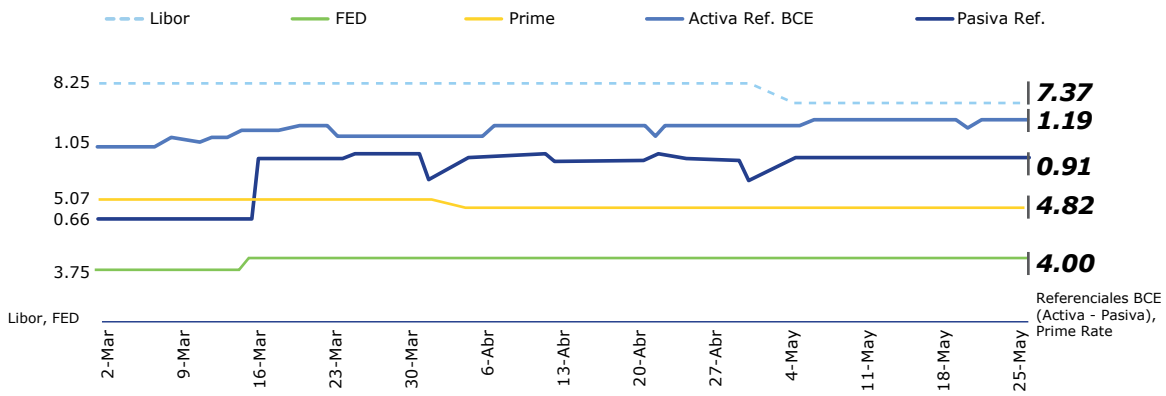
Monedas	Cotización Internacional	Tasa Oficial	Transacciones	
			Compra	Venta
Bolívar Fuerte	10.11	10.12	6.29	6.29
Euro	0.89	0.89	0.94	0.94
Libra Esterlina	0.77	0.77	0.66	0.66
Nuevo Sol	3.27	3.28	3.39	3.39
Peso argentino	16.10	16.10	9.68	9.68
Peso boliviano	6.86	6.91	6.90	6.90
Peso chileno	673.95	675.68	714.29	714.29
Peso colombiano	2904.44	2941.18	3125.00	3125.00
Real	3.27	3.27	3.77	3.77
Yen	112.01	111.98	122.70	122.70

Valores expresan unidades de cada moneda que se obtienen por cada $US

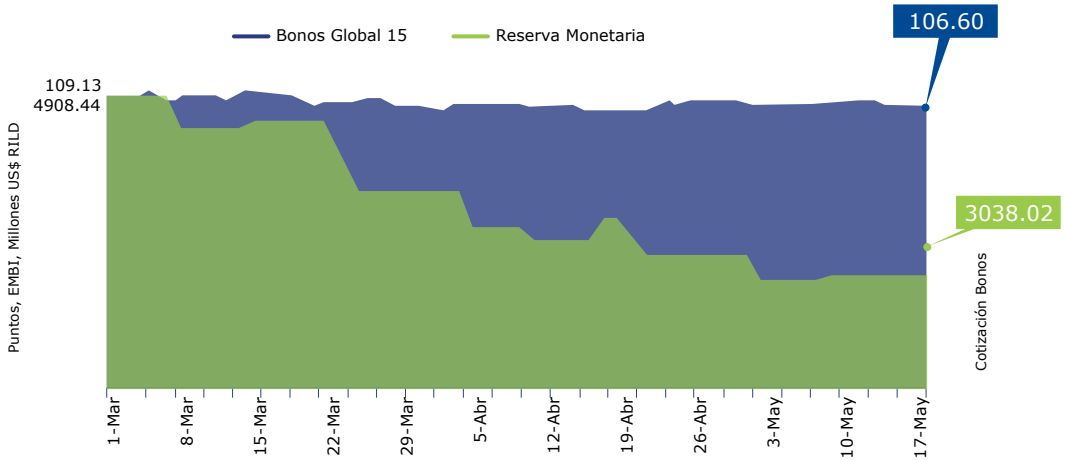
Evolución de Indicadores



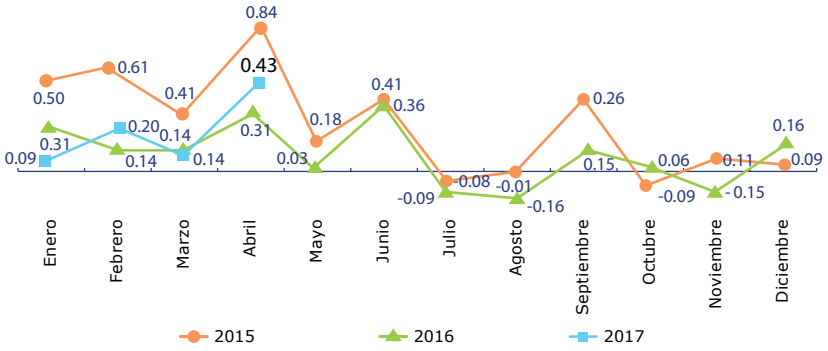
Tasas Referenciales



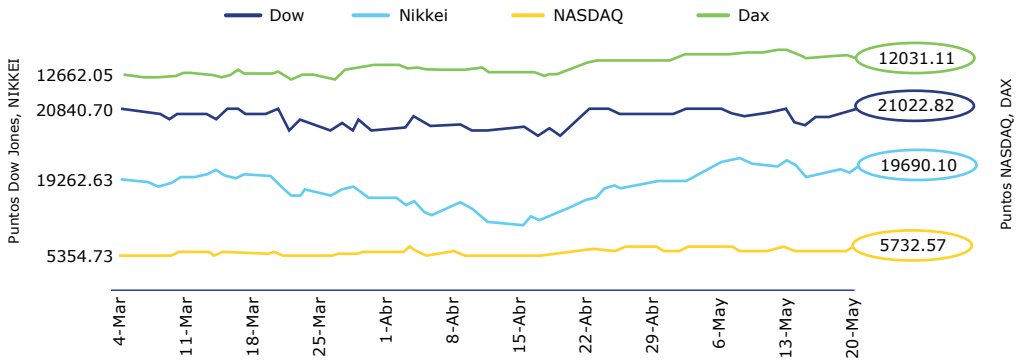
Bonos Global 15 y RILD



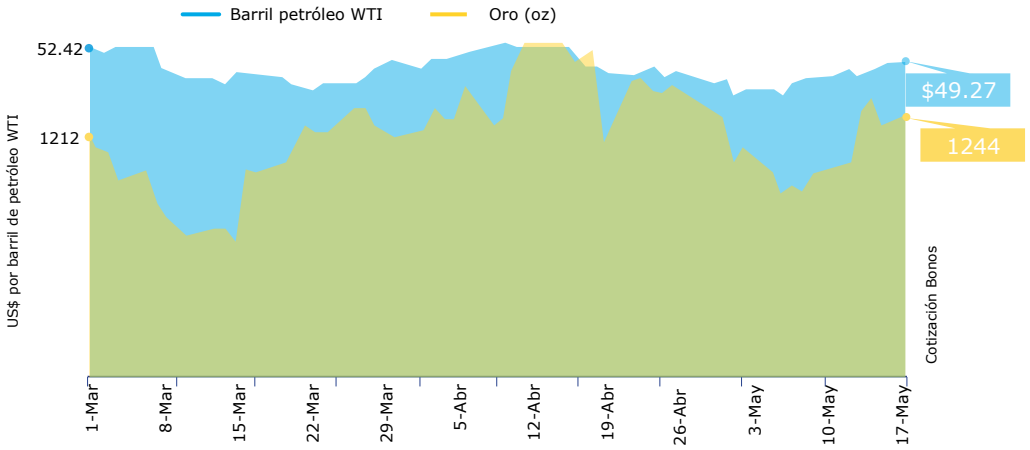
Inflación



Índices Bursátiles



Materias Primas



Tasas de interés referenciales					Internacionales				
Período	Básica del Banco Central	Pasiva Referencial	Activa Referencial	Legal	Prime NY	Libor			
						30 días	60 días	180 días	360 días
2012	0.20	4.53	8.17	8.17	3.25	0.21	0.31	0.51	0.84
2013	0.20	4.53	8.17	8.17	3.25	0.19	0.26	0.41	0.68
2014	0.20	5.18	8.19	8.19	3.25	0.16	0.24	0.34	0.60
2015	0.20	5.62	9.15	9.15	3.25	0.42	0.60	0.83	1.15
2016	0.20	5.12	8.10	8.10	3.75	0.77	1.00	1.32	1.69
Enero 2017	0.20	5.08	8.02	8.02	3.75	0.77	0.85	1.35	1.71
Febrero 2017	0.20	5.07	8.25	8.25	3.75	0.78	0.85	1.36	1.75
Marzo 2017	0.20	4.98	8.14	8.14	4.00	0.98	1.15	1.43	1.80
Abril 2017	0.20	4.81	8.13	8.13	4.00	0.99	1.16	1.40	1.74
Mayo 2017	0.20	4.82	7.37	7.37	4.00	1.02	1.19	1.41	1.72

Fuente: Banco Central del Ecuador

Tasas de interés activas efectivas calculadas por el Banco Central

Segmento de Crédito				
	Productivo Corporativo	Tasa Referencial: 9.61% Tasa Máxima: 9.33%	**Productivo PYMES**	Tasa Referencial: 11.49% Tasa Máxima: 11.83%
	Consumo	Tasa Referencial: 16.80% Tasa Máxima: 17.30%	**Vivienda**	Tasa Referencial: 10.61% Tasa Máxima: 11.33%
	Microcrédito acumulación ampliada	Tasa Referencial: 21.42% Tasa Máxima: 25.50%		

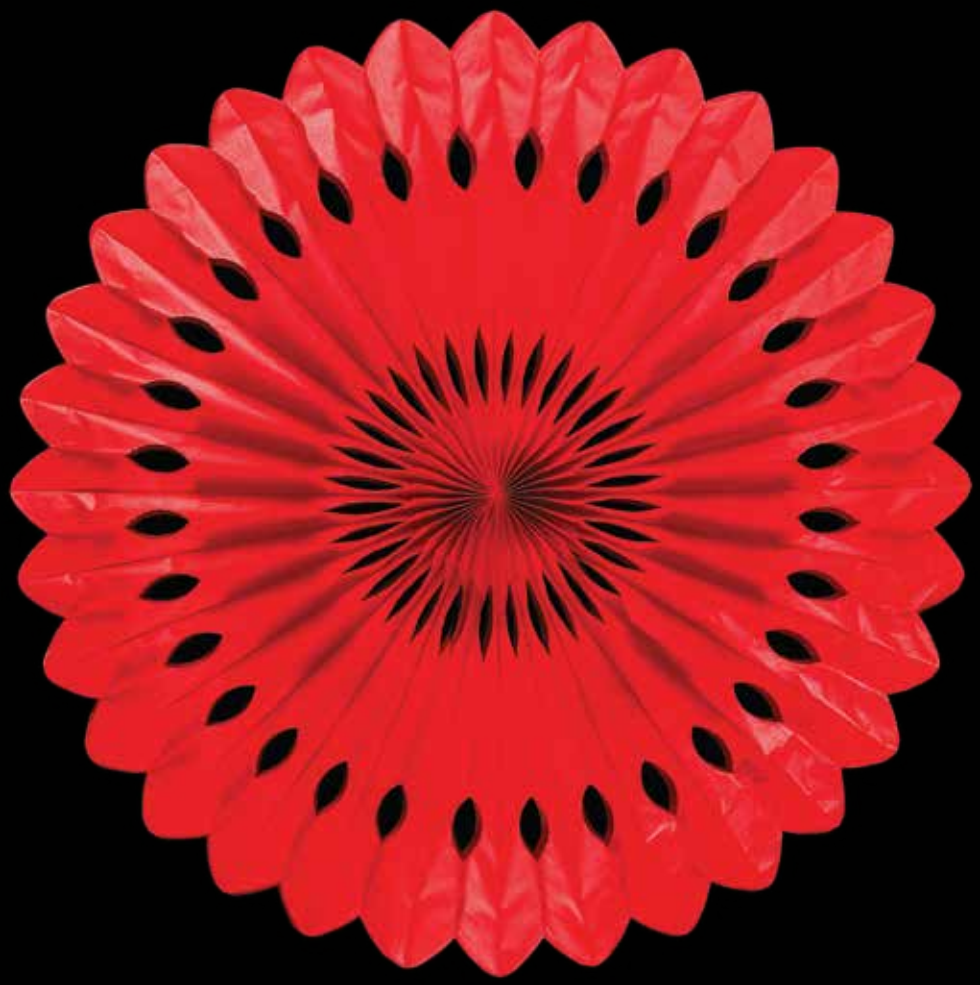
Fuente: Banco Central del Ecuador

Evaluación de la inflación

	2015					2016					2017				
	% INFLACIÓN					% INFLACIÓN					% INFLACIÓN				
	INDICE	MES	ACUMULADA (Por el año)	ANUAL (12 meses)	ANUALIZADA (Mes * 12)	INDICE	MES	ACUMULADA (Por el año)	ANUAL (12 meses)	ANUALIZADA (Mes * 12)	INDICE	MES	ACUMULADA (Por el año)	ANUAL (12 meses)	ANUALIZADA (Mes * 12)
Enero	101.24	0.59	0.59	3.53	7.39	104.37	0.31	0.31	3.09	3.75	105.30	0.09	0.09	0.90	1.03
Febrero	101.86	0.61	1.21	4.05	7.60	104.51	0.14	0.45	2.60	1.62	105.51	0.20	0.29	0.96	2.42
Marzo	102.28	0.41	1.63	3.76	5.06	104.65	0.14	0.58	2.32	1.62	105.66	0.14	0.42	0.96	1.72
Abril	103.14	0.84	2.48	4.32	10.57	104.97	0.31	0.89	1.78	3.73	106.12	0.43	0.86	1.09	5.35
Mayo	103.32	0.18	2.66	4.55	2.11	105.01	0.03	0.92	1.63	0.46					
Junio	103.74	0.41	3.08	4.87	4.99	105.38	0.36	1.29	1.59	4.31					
Julio	103.66	-0.08	2.99	4.36	-0.92	105.29	-0.09	1.20	1.58	-1.02					
Agosto	103.65	-0.01	2.99	4.14	-0.12	105.12	-0.16	1.04	1.42	-1.92					
Septiembre	103.93	0.26	3.27	3.78	3.29	105.28	0.15	1.19	1.30	1.84					
Octubre	103.84	-0.09	3.17	3.48	-1.03	105.20	-0.06	1.11	1.31	-0.91					
Noviembre	103.95	0.11	3.28	3.40	1.28	105.04	-0.15	0.96	1.05	-1.81					
Diciembre	104.05	0.09	3.38	3.38	1.16	105.21	0.16	1.12	1.12	1.96					

* Nuevas bases ene2014: 98.81 y dic14: 100.32 * Año 2005, Año 2006 valores corregidos
**Los índices del IPC (Base: 2004=100) han sido empalmados a la serie del nuevo IPC (Base: 2014=100).

Deloitte.



50 años siendo líderes

www.deloitte.com/ec