1.10.1 Seguridad de la información / Gobernanza de la ciberseguridad

¿Está el consejo de administración involucrado en la estrategia de seguridad de la información / ciberseguridad y en el proceso de revisión? ¿La persona responsable de TI tiene antecedentes relevantes en cuanto a seguridad de la información o ciberseguridad?

Sí está involucrado. A través del Comité de Auditoría y del mismo Consejo de Administración que anualmente realiza el proceso de revisión.

Se les presentan las medidas de seguridad que se tienen implementadas en el acceso a la red, ellos tienen conocimiento de lo que se está realizando en el área.

Yes, he is involved. Through the Audit Committee and the same Board of Directors that annually performs the review process.

They are presented with the security measures that are implemented in the access to the network, they have knowledge of what is being done in the area.

❍ Sí, el Consejo está involucrado en el proceso de la estrategia de ciberseguridad y la persona responsable de TI cuenta con background suficiente. Por favor adjunte los documentos de apoyo pertinentes.

Sí, hay políticas y procedimientos públicos y que se revisan periódicamente para asegurar su adecuada difusión y vigencia. También se cuenta con procedimientos en intranet de la compañía.

Yes, there are public policies and procedures that are reviewed periodically to ensure their proper dissemination and validity. There are also procedures on the company's intranet.

Por favor indique el nombre y el curriculum de la (s) persona (s) responsable (s):

Ing. Carlos Conss Curiel (Sub Director de Servicios de Información)

El Sr. Conss Curiel ingresó a KCM en 1981 y ocupa el puesto de Subdirector de Servicios de Información desde 2000. Otros puestos que ha ocupado incluyen Gerente de Servicios de Información y Gerente de Desarrollo de Sistemas. El Sr. Conss Curiel es Licenciado en Administración por la Universidad de las Américas, tiene Maestría en Economía y Negocios por la Universidad Anáhuac y ha laborado 37 años en la Compañía.

Ing. Carlos Conss Curiel (Assistant Director of Information Services)

Mr. Conss Curiel joined KCM in 1981 and holds the position of Deputy Director of Information Services since 2000. Other positions he has held include Information Services Manager and Systems Development Manager. Mr. Conss Curiel has a Bachelor's Degree in Business Administration from the

University of the Americas, a Master's Degree in Economics and Business from Universidad Anáhuac and has worked for the company for 37 years.

1.10.2 Medidas de seguridad

¿Ha implementado políticas y procedimientos para empleados con acceso a información crítica a fin de garantizar que estén consciente de los problemas de amenazas y de la importancia de la seguridad de la información / la seguridad informática?

❍ Sí, hemos implementado políticas y procedimientos para empleados con acceso a información crítica.

❑ Una política de seguridad de la información / ciberseguridad está disponible internamente para todos los empleados, proporcione el documento:

❑ Formación en concientización sobre seguridad de la información / ciberseguridad. Por favor explique y proporcione evidencia de apoyo:

_ _

❑ Existe un proceso de escalado claro que los empleados pueden seguir en el caso de que un empleado note que hay algo sospechoso.

Hay un reporte de incidente crítico, a través de un correo electrónico dirigido a las gerencias y direcciones que tengan injerencia en el tema.

There is a critical incident report, through an email addressed to the managements and addresses that have interference in the subject.

Por favor explique y proporcione evidencia de apoyo:

_ _

❑ La seguridad de la información / la ciberseguridad forma parte de la evaluación del desempeño del empleado (por ejemplo, acciones disciplinarias). Por favor explique y proporcionar evidencia de apoyo:

1.10.3 Proceso e Infraestructura

Esta pregunta evalúa si las empresas cuentan con los procesos correctos para evitar interrupciones del sistema de TI y ataques cibernéticos y si están bien preparados para reaccionar en caso de tales eventos.

❍ **Respuesta a incidentes**

¿Tiene implementados planes de continuidad / contingencia de negocios y procedimientos de respuesta a incidentes y con qué frecuencia los prueba?

Por favor proporcione evidencia de apoyo.

❍ Sí, y los probamos al menos semestralmente.

❍ Sí, y los probamos al menos una vez al año.

Hacemos una prueba de que todas nuestras aplicaciones de negocios puedan operar en un site alterno, es un servicio proporcionado por IBM México. Además nuestro socio estratégico KCC cuenta con dos centros de datos que respaldan en automático la información y aplicaciones de negocios con los que nosotros contamos

We make a proof that all our business applications can operate in an alternate site, it is a service provided by IBM Mexico. In addition, our strategic partner KCC has two data centers that automatically support the information and business applications that we have.

❍ Sí, pero pruébalos con menos frecuencia

❍ No, no tenemos dichos planes y procedimientos establecidos

Certificación

¿Su sistema de gestión de seguridad de la información y la infraestructura de TI está certificado según ISO 27001, NIST o similar?

❍ Sí, el siguiente porcentaje de nuestra infraestructura de TI ha sido certificado:

_ _ _ _ _ _ _ _ _

❍ No, nuestra infraestructura de TI no ha sido certificada.

No, lo que hacemos es seguir las normas de nuestro socio estratégico KCC ya que nosotros movemos nuestra infraestructura a su sitio corporativo. Ellos a su vez, cumplen con las políticas de gobierno corporativo impuestas globalmente. Para dar un ejemplo, se siguen los lineamientos que marcan la SEC Sabarnes & Oxley

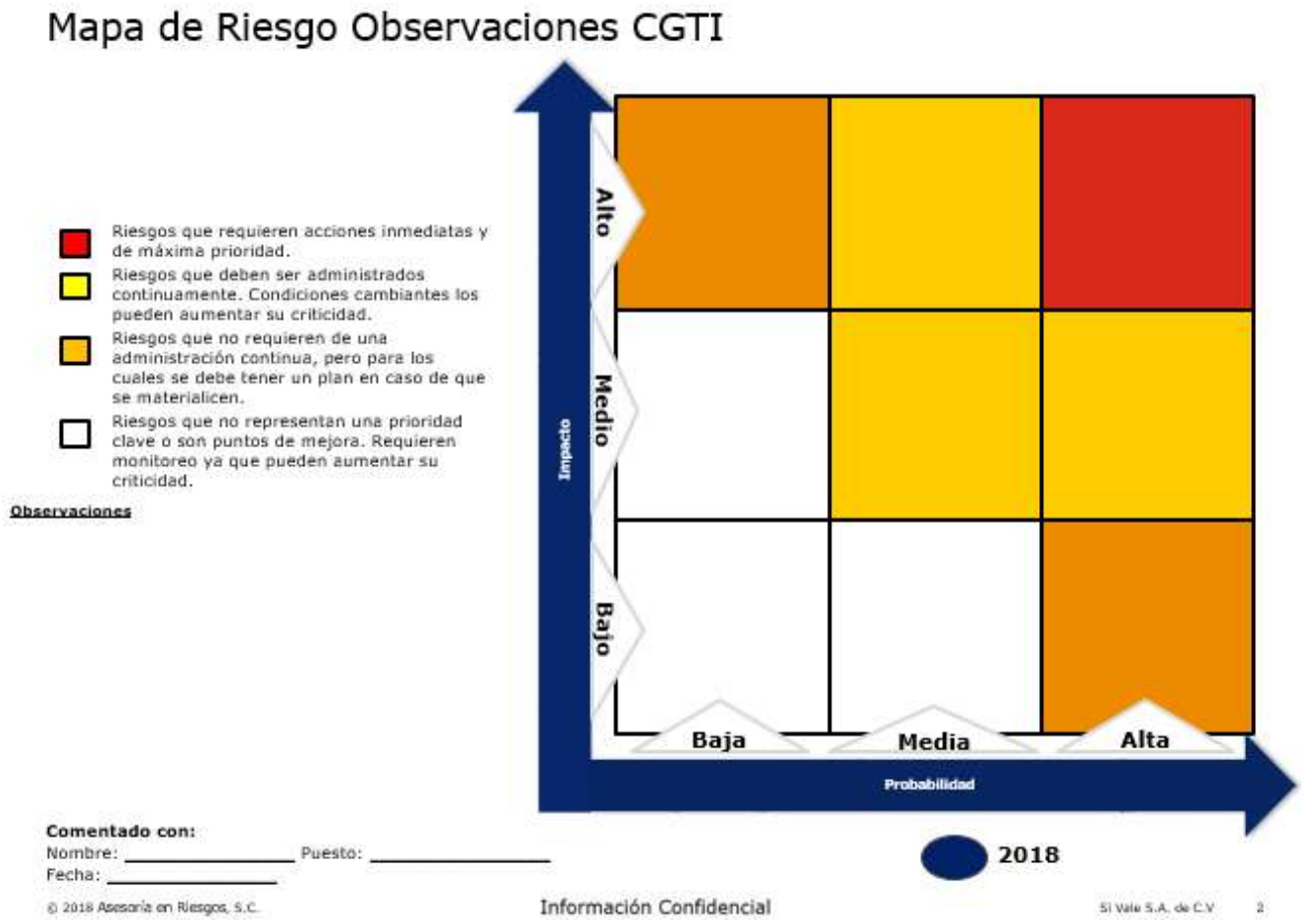
No, what we do is follow the rules of our strategic partner KCC as we move our infrastructure to your corporate site. They, in turn, comply with the corporate governance policies imposed globally. To give an example, follow the guidelines set by SEC Sabarnes & Oxley

Verificación externa y análisis de vulnerabilidad

Indique si hay otros procedimientos adicionales implementados para garantizar la seguridad de la infraestructura / información del sistema de gestión de seguridad de TI. Por favor proporcione la declaración de auditoría o informe.

Deloitte audita nuestros procedimientos adicionales implementados para garantizar la seguridad de nuestra infraestructura.

Deloitte audits our additional procedures implemented to ensure the security of our infrastructure.



Cabe señalar que en este informe de Deloitte, se felicita a KCM por no haber encontrado deficiencias.

It should be noted that in this Deloitte report, KCM is congratulated for not finding deficiencies.

❑ Nuestros sistemas de gestión de seguridad de la información y la infraestructura de TI han sido auditados por auditores externos en el último ejercicio año fiscal. Por favor proporcione una carta de opinión del auditor externo.

❑ Hacemos análisis de vulnerabilidad incluyendo ataques de hackers simulados. Por favor describa:

_ _

❍ No contamos con procesos ni infraestructura para prevenir y / o responder a ataques cibernéticos.

❍ No aplicable. Sírvanse proporcionar explicaciones en el espacio de comentarios a continuación.

Los ejecuta la corporación pero nosotros no tenemos una participación directa.

❍ No se sabe

1.10.4 Seguridad de la información / violaciones de la ciberseguridad

Esta pregunta evalúa el éxito de su empresa en la gestión de los riesgos de seguridad de la información / ciberseguridad en los últimos tres años y cuál fue el impacto financiero. La segunda parte de la pregunta evalúa cómo se mitiga el riesgo financiero a través de seguro.

❍ Moneda:

_ _ _ _ _ _ _ _ _

Incidentes y violaciones

¿Su empresa ha experimentado violaciones de seguridad de la información u otros incidentes de seguridad informática en los últimos tres años?

Ninguno

None

Tenga en cuenta que si no tuvo ninguna infracción de información, multas o responsabilidad acumulada en un año individual, debe ingresar 0

En la casilla correspondiente de la tabla. Si no conoce la información, deje la casilla en blanco. Ver el texto informativo para más información.

	2016	2017	2018
Número total de violaciones a la información de seguridad u otros incidentes de ciberseguridad	0	0	0
Número total de violaciones a la información de seguridad que involucran	0	0	0

información personal de clientes			
Importe total de las multas / sanciones pagadas en relación a violaciones de seguridad de la información u otro incidente de ciberseguridad.	0	0	0

Seguro Contra Incumplimientos

¿Tiene cobertura de seguro para violaciones de seguridad de la información u otros incidentes de ciberseguridad?

❍ Sí, tenemos una póliza de seguro con una cobertura máxima de:

_ _ _ _ _ _ _ _ _

❍ No, no tenemos cobertura de seguro.

No. En las pólizas está excluido el software por ser algo intangible, no es objeto de cobertura de las pólizas vigentes. Al ser un riesgo emergente recientemente hicimos un análisis de lo que ofrecen las aseguradoras pero aún no contamos con póliza de seguro para este riesgo, estamos evaluando las opciones de transferencia de riesgo con los productos que están actualmente en el mercado.

No. In the policies the software is excluded because it is something intangible, it is not covered by the current policies. Being an emerging risk, we recently made an analysis of what the insurers offer but we still do not have an insurance policy for this risk, we are evaluating the risk transfer options with the products that are currently on the market.

❍ No recopilamos datos sobre violaciones de seguridad de la información / ciberseguridad e incidentes.

❍ No aplicable. Sírvanse proporcionar explicaciones en el espacio de comentarios a continuación.