INSTRUCTIVO PARA LA PROTECCIÓN DE DATOS PERSONALES

ANTECEDENTES

La Ley Orgánica de Protección de Datos Personales fue expedida por la Asamblea Nacional del Ecuador y entró en vigencia a partir de su publicación en el Registro Oficial – Quinto Suplemento No 459 con fecha miércoles 26 de mayo de 2021. A partir del 26 de mayo de 2023 inició la aplicación del régimen sancionatorio de esta ley que contempla multas que van desde el 0.7% hasta el 1% de la facturación de una empresa pública o privada, aparte de indemnizaciones por daños y perjuicios a personas afectadas por el mal uso de sus datos personales.

ÁMBITO DE APLICACIÓN INTEGRAL

El objetivo de la presente ley es garantizar el ejercicio del derecho de protección de datos personales, que incluye el **acceso y decisión sobre información de datos** de este carácter, así como su correspondiente **protección**. Aplica al tratamiento de datos personales: a) **contenidos en cualquier tipo de soporte**, automatizados o no, así como a toda modalidad de uso posterior, b) que se realice en cualquier parte del territorio nacional. A continuación, se indican los términos y definiciones más relevantes de la esta ley:

1) **Dato personal**: dato que identifica o hace identificable a una **persona natural**, directa o indirectamente. La clasificación de datos personales establecida es la siguiente:

   a) **Dato biométrico**: características físicas o fisiológicas, ej. imágenes faciales o datos dactiloscópicos.
   b) **Dato genético:** características genéticas heredadas o adquiridas.
   c) **Datos crediticios:** comportamiento económico.
   d) **Datos de salud:** física o mental, prestación de servicios médicos, estado de salud.
   e) **Datos sensibles:** etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atente o puedan atentar contra los derechos y libertades fundamentales.
   f) **Datos especiales:** datos sensibles; datos de niñas, niños y adolescentes; datos de salud; datos de personas con discapacidad y de sus sustitutos, relativos a la discapacidad.
   g) **Datos de personas fallecidas.**

2) **Tratamiento**: cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, **cualquier uso de datos personales**.

   El tratamiento de datos personales será **legítimo y lícito** si se cumple con **alguna** de las siguientes **condiciones**:
   a) Por **consentimiento del titular** para el tratamiento de sus datos personales, para una o varias finalidades específicas;
   b) Que sea realizado por el responsable del tratamiento en cumplimiento de: una obligación legal, una orden judicial, una misión realizada en interés público;
   c) Para la ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales perseguidas por el responsable o el encargado del tratamiento de datos personales o por un tercero legalmente habilitado;
   d) Para proteger intereses vitales del interesado o de otra persona natural, como su vida o integridad;
   e) Para tratamiento de datos personales que consten en bases de datos de acceso público;
   f) Para satisfacer un interés legítimo del responsable del tratamiento o de un tercero, siempre que no prevalezca el interés o derechos fundamentales de los titulares al amparo de lo dispuesto en esta norma.

3) **Consentimiento**: se podrán tratar y comunicar datos personales **cuando se cuente con la manifestación de la voluntad del titular** para hacerlo. El consentimiento será válido cuando la manifestación de la voluntad sea:

   a) Libre, es decir, cuando se encuentre exenta de vicios del consentimiento;
   b) Específica, en cuanto a la determinación concreta de los medios y fines de tratamiento;
   c) Informada, de modo que cumpla con el principio de transparencia y efectivice el derecho a la transparencia;
   d) Inequívoca, de manera que no presente dudas sobre el alcance de la autorización otorgada por el titular.

   El consentimiento podrá revocarse en cualquier momento sin que sea necesaria una justificación, para lo cual el responsable del tratamiento de datos personales establecerá mecanismos que garanticen celeridad, eficiencia, eficacia y gratuidad, así como un procedimiento sencillo, similar al proceder con el cual recabó el consentimiento.

4) **Integrantes del sistema de protección de datos personales:** son parte del sistema de protección de datos personales los siguientes:

   a) **Titular:** persona natural cuyos datos son objeto de tratamiento.
   b) **Responsable del tratamiento:** persona natural o jurídica que decide sobre la finalidad y el tratamiento de datos personales.
   c) **Encargado del tratamiento:** persona natural o jurídica que trata datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales.
   d) **Destinatario:** quien ha sido comunicado con datos personales.
   e) **Autoridad de protección de datos personales:** autoridad pública que protege los derechos y libertades de las personas naturales, en cuanto al tratamiento de sus datos personales.
   f) **Delegado de protección de datos personales:** persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la autoridad de protección de datos personales, sirviendo como punto de contacto entre ésta y la entidad responsable de tratamiento de datos.

5) **Vulneración de la seguridad de datos personales:** incidente de seguridad que afecta la **confidencialidad, disponibilidad o integralidad** de los datos personales.

PRINCIPIOS

Los principios que rigen el tratamiento de datos personales son: a) juridicidad, b) lealtad, c) transparencia, d) finalidad, e) pertinencia y minimización de datos personales, f) proporcionalidad del tratamiento, g) confidencialidad, h) calidad y exactitud, i) conservación, j) seguridad de datos personales, k) responsabilidad proactiva y demostrada, l) aplicación favorable al titular, m) independencia del control.

DERECHOS

A continuación, se resumen los derechos de los titulares de datos personales:

1) Aplicación de la normativa especializada para el tratamiento de datos personales.

2) Derecho a la información, esto es para el caso de nuestra empresa:

a) **Los fines del tratamiento:**

- En el área de marketing y ventas: calificación de solicitudes de distribución de Helados Los Coqueiros (se solicita adjuntar copias de cédula, RUC y planilla de energía eléctrica del domicilio, y autorización para revisar información en el buró de crédito), elaboración de contratos de comodato de congeladores y recibos de publicidad, emisión de facturas y notas de crédito, registro en base de datos de clientes y ruteros, envío de comunicaciones de la empresa, envío de publicidad, aplicación de encuestas.

- En todas las áreas de la empresa: calificación de proveedores (se solicita carta de presentación, copia de cédula, RUC, certificaciones de calidad, proformas), elaboración de contratos cuando aplica, emisión de retenciones, emisión de pagos, registro en base de datos de proveedores, envío de comunicaciones de la empresa, aplicación de encuestas.

- En el área de talento humano y seguridad y salud ocupacional: calificación de solicitudes de empleo (se solicita adjuntar hoja de vida, acreditaciones y autorización para revisar información en el buró de crédito), elaboración de contratos de trabajo, emisión de pagos, registro en nómina, envío de comunicaciones de la empresa, aplicación de encuestas, realización de exámenes médicos pre-ocupacionales, ocupacionales y de retiro.

b) La base legal para el tratamiento: la Ley Orgánica de Protección de Datos Personales.

c) Tipos de tratamiento:

- Tratamiento comercial para el caso de clientes y proveedores.
- Tratamiento administrativo para el caso del personal de la empresa.

d) Tiempo de conservación:

- Datos personales de clientes y proveedores: por el tiempo que dure la relación comercial y hasta dos años después de su conclusión como archivo histórico con fines de trazabilidad y posible recalificación.

- Datos personales de trabajadores: por el tiempo que dure la relación laboral y de manera permanente como archivo histórico con fines de consulta y posible recontratación.

- Para el caso de clientes potenciales, proveedores potenciales y trabajadores potenciales que no superen el proceso de calificación, su información será descartada dentro de los dos meses posteriores a la conclusión del proceso en mención.

e) La existencia de una base de datos en la que constan sus datos personales: existe para el caso de clientes, proveedores y trabajadores actuales.

f) El origen de los datos personales cuando no se hayan obtenido directamente del titular: búsqueda de información en internet publicada por el mismo titular o por entidades u otras fuentes en general relacionadas con el mismo, selección de datos personales por algoritmos utilizados en el ecosistema digital e interacción en redes sociales.

g) Otras finalidades y tratamiento ulteriores: solo aplican las indicadas en el literal a).

h) **Identidad y datos del contacto responsable del tratamiento de datos personales:** Heladerías Cofrunat Cía. Ltda., El Morlán N52-18 e Isaac Barrera, 02 241 5594 – 5595, correo para la atención de consultas sobre la política de protección de datos personales de la empresa: info@loscoqueiros.com

i) Cuando sea del caso, identidad y datos del contacto del delegado de protección de datos personales: jefatura de cada unidad estratégica.

j) Las transferencias o comunicaciones, nacionales e internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y sus clases, así como las finalidades que motivan la realización de estas y las garantías de protección establecidas.

k) Las consecuencias para el titular de los datos personales de su entrega o negativa a ello: para el caso de la entrega se agilitarán los procesos de calificación; y, para el caso de su no entrega la falta de información requerida generará demora y afectación a los procesos de calificación.

l) El efecto de suministrar datos personales erróneos o inexactos: afectación a procesos de calificación por falta de confiabilidad en la información proporcionada.

m) **La posibilidad de revocar el consentimiento:** el titular podrá revocar en el momento en que desee el consentimiento dado a la empresa para el tratamiento de sus datos personales **comunicando su voluntad por escrito** a través del envío de un correo electrónico a info@loscoqueiros.com y/o a través del envío de un mensaje de texto o correo electrónico al puesto de trabajo a cargo de su atención.

n) La existencia y forma en que pueden hacerse efectivos sus derechos de acceso, eliminación, rectificación y actualización, oposición, anulación, limitación del tratamiento y a no ser objeto de una decisión basada únicamente en valoraciones automatizadas: aplica el procedimiento indicado en el literal m).

o) Los mecanismos para hacer efectivo su derecho a la portabilidad, cuando el titular lo solicite: aplica el procedimiento indicado en el literal m).

p) Dónde y cómo realizar los reclamos ante el responsable del tratamiento de datos personales y la Autoridad de Protección de Datos Personales: aplica el procedimiento indicado en el literal m). Todo reclamo será puesto en conocimiento del gerente general de la empresa para asegurar el tratamiento adecuado de cada caso. Los reclamos ante la autoridad competente deberán seguir el procedimiento establecido por la misma entidad.

q) La existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles: no existen.

La **comunicación** de la información correspondiente a la **política de protección de datos personales de Heladerías Cofrunat Cía. Ltda.** para conocimiento del titular de datos personales y de todo interesado se realizará a través de su publicación en la página web de la empresa https://www.loscoqueiros.com Las consultas sobre la política en mención serán recibidas a través del correo electrónico info@loscoqueiros.com

3) Derecho de acceso: el titular podrá solicitar a la empresa el acceso a su información de datos personales de manera gratuita a través del envío de un correo electrónico a info@loscoqueiros.com y/o a través del envío de un mensaje de texto o correo electrónico al puesto de trabajo a cargo de su atención. La empresa tendrá la obligación de proporcionar la información solicitada dentro de los 15 días siguientes a la recepción de su solicitud.

4) Derecho de rectificación y actualización: aplica el procedimiento indicado en el numeral 3).

5) Derecho de eliminación: aplica el procedimiento indicado en el numeral 3).

6) Derecho de oposición: aplica el procedimiento indicado en el numeral 3).

7) Derecho a la portabilidad.

8) Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad.

9) Derecho a la suspensión del tratamiento.

10) Derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas.

11) Derecho de niñas, niños y adolescentes a no ser objeto de una decisión basada única y parcialmente en decisiones automatizadas.

12) Derecho de consulta.

13) Derecho a la educación digital.

14) Ejercicio de derechos.

SEGURIDAD DE DATOS PERSONALES

El responsable o encargado del tratamiento de datos personales deberá:

- Realizar un análisis de riesgos, amenazas y vulnerabilidades.
- Determinar las medidas de seguridad aplicables.
- Verificar, evaluar y valorar continua y permanentemente la eficiencia, eficacia y efectividad de las medidas de seguridad aplicables (de carácter técnico, organizativo o de cualquier otra índole) con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales, y evidenciar que mitigan de forma adecuada los riesgos identificados.
- Notificar la vulneración de seguridad.

A continuación, se presenta la realización de las actividades indicadas:

1) Realizar un análisis de riesgos, amenazas y vulnerabilidades.

Antes de realizar este análisis es importante tener claras las categorías y volumen de datos personales, los lugares de almacenamiento y las formas en las que éstos podrían ser sustraídos.

a) Categorías de datos personales:

- Categoría 1: datos personales de clientes potenciales, activos e inactivos. Custodio: Asistentes de Ventas.
- Categoría 2: datos personales de trabajadores potenciales, activos e inactivos. Custodio: Jefe de Talento Humano y Seguridad y Salud Ocupacional, excepto los datos de salud los cuales serán manejados exclusivamente por la Médico Ocupacional Externa.
- Categoría 3: datos personales de proveedores con personería natural potenciales, activos e inactivos. Custodio: Auxiliares Contables.

b) Volumen de datos personales:

- Categoría 1: documentos firmados: solicitud de distribución con consentimiento para el tratamiento de datos personales y autorización para la revisión de información crediticia en el buró de crédito; documentos adjuntos: copia de cédula, copia de RUC, copia de planilla de energía eléctrica de domicilio y/o local comercial; reporte de investigación de referencias; otros documentos firmados: contrato de comodato por el congelador, recibo de publicidad; información bancaria: para pago de notas de crédito.

- Categoría 2: hoja de vida con certificados varios adjuntos; documentos firmados: solicitud de empleo con consentimiento para el tratamiento de datos personales, autorización para la revisión de información crediticia en el buró de crédito; otros documentos adjuntos: copia de cédula, copia de licencia de conducir, copia de planilla de energía eléctrica de domicilio; reporte de investigación de referencias; información bancaria: para pago de remuneraciones; otros documentos firmados: autorizaciones de descuento, amonestaciones; información médica: para control y seguimiento de estado de salud mediante exámenes pre-ocupacionales, ocupacionales y de retiro.

- Categoría 3: carta de presentación, hoja de vida con certificados varios adjuntos para los casos que aplique, certificado de afiliación al IESS; documentos firmados: solicitud de proveedor con consentimiento para el tratamiento de datos personales, contratos para los casos que aplique; reporte de investigación de referencias; información bancaria: paga pago de facturas.

c) Lugares de almacenamiento de datos personales:

- Categoría 1: a) archivo físico de documentación de clientes en mobiliario del área de ventas: archivo de documentos de clientes activos, archivo de documentos de clientes inactivos; archivo de facturas por cobrar y cobradas; b) registro digital de información de clientes en computadores del personal del área de ventas: bases de datos en Microsoft Office y en programa contable QuickBooks.

- Categoría 2: a) archivo físico de documentación del personal en mobiliario del área de talento humano y seguridad y salud ocupacional, y en el área de atención médica: files de trabajadores actuales y ex – trabajadores y documentos de candidatos; historias clínicas de trabajadores actuales y ex – trabajadores; b) registro digital de información del personal en computadores del personal del área de talento humano y seguridad ocupacional y del área de atención médica: bases de datos en Microsoft Office y en programa contable QuickBooks.

- Categoría 3: a) archivo físico de documentación de proveedores – personas naturales en mobiliario del área de contabilidad y auditoría: files de proveedores, files de contratos; b) registro digital de información de proveedores – personas naturales en computadores del personal del área de contabilidad y auditoría: bases de datos en Microsoft Office y en programa contable QuickBooks.

d) Formas en las que los datos personales podrían ser sustraídos:

Ahora que se tienen claras las categorías y volumen de datos personales y los lugares de almacenamiento, a continuación, se realiza un análisis de riesgos, amenazas y vulnerabilidades para determinar las formas en las que éstos podrían ser sustraídos:

Riesgos: se denomina riesgo a la posibilidad de que un sistema sufra un incidente de seguridad y que una amenaza se materialice causando una serie de daños.

Para medir el riesgo de un sistema se debe asumir que existe una vulnerabilidad ante una amenaza. El riesgo es, por lo tanto, la probabilidad de que la amenaza se materialice aprovechando una vulnerabilidad existente.

- Para todas las categorías de datos se considera que existe un riesgo medio ante las amenazas causadas por ataques informáticos y un riesgo bajo ante las amenazas causadas por sucesos inesperados en función de las vulnerabilidades actuales de la empresa.

Amenazas: una amenaza es la posibilidad de que un sistema vulnerable sea atacado y sufra daños.

- Para todas las categorías de datos se considera que la principal amenaza es la sustracción de datos personales con fines delincuenciales siendo el más relevante la suplantación de identidad a través de: la usurpación de la cédula de identidad, robo de firma, suplantación digital, tarjetas de crédito, estafas telefónicas, usurpación de identidad en redes sociales. Las principales consecuencias del robo de identidad son: pérdida de reputación, pérdida de ingresos, pérdida financiera, pérdida de propiedad intelectual.

  Por tanto, los datos personales que más se deben cuidar son los nombres completos, el número de cédula, la fecha de nacimiento, números de teléfono, direcciones físicas, direcciones electrónicas, ubicaciones, datos sensibles. Adicionalmente, cualquier tipo de información comprometedora que

pudiera llegar a estar en los archivos de la empresa por algún motivo. Ejemplo: fotos comprometedoras, fotos de menores, conversaciones privadas, etc.

Se destacan dos tipos de amenazas principales: amenazas causadas por ataques informáticos y amenazas causados por sucesos inesperados. A continuación, se explica brevemente cada una:

- ✓ **Amenazas causadas por ataques informáticos:** las amenazas de un sistema informático provienen principalmente de ataques externos (malware, denegación de servicio o inyecciones SQL, entre otros), de no cumplir las políticas de seguridad (conectar dispositivos no autorizados a la red o utilizar contraseñas débiles). Las amenazas más importantes a las que se enfrenta una infraestructura IT (tecnologías de la información) son:

  - Código malicioso. Estos ataques malware atacan dispositivos y servidores con el fin de robar información sensible, como datos bancarios o credenciales de acceso. Los ataques ransomware son una de las mayores amenazas hoy en día para los sistemas informáticos de las empresas.

  - Robo de identidad. Otra amenaza que pone en riesgo los sistemas de una organización es el phishing o robo de identidad. La amenaza consiste en engañar al usuario para que facilite de forma involuntaria sus credenciales de acceso a un tercero que las utilizará de forma fraudulenta.

  - Amenazas Persistentes Avanzadas. Las conocidas como APT (Amenazas Persistentes Avanzadas) son ataques coordinados que se dirigen a una empresa para robar sus datos. Son una de las amenazas más difíciles de detectar, ya que utilizan técnicas de ingeniería social.

  - Denegación de servicio. Los ataques DDoS son una amenaza que se cierne sobre servidores que pretenden ser colapsados enviándoles una enorme cantidad de peticiones (haciendo que no puedan atenderlas, e incluso que terminen cayendo).

  - Negligencia. Los usuarios suelen ser la mayor amenaza para un sistema informático. Los errores humanos y el no incumplimiento de las políticas y normas de seguridad de la empresa ponen en peligro los sistemas y los datos de la empresa.

- **Amenazas causadas por sucesos inesperados:** como incendios o robos físicos, por ejemplo. Incluye sustracción o pérdida de información relacionada con datos de personas naturales por parte del mismo personal de la empresa de forma intencional y no intencional.

Vulnerabilidades: se considera una vulnerabilidad a una debilidad propia de un sistema que permite ser atacado y recibir un daño.

Para el caso de los sistemas informáticos, las vulnerabilidades se producen de forma habitual por una baja protección contra ataques externos, falta de actualizaciones, fallos de programación, y otras causas similares. A las vulnerabilidades también se las conoce como agujeros de seguridad y tienen la ventaja de que pueden ser solventadas una vez sean descubiertas.

Una vulnerabilidad pone en riesgo los datos y sistemas de una empresa comprometiendo su integridad, privacidad y disponibilidad.

- Para todas las categorías de datos se han ubicado las principales vulnerabilidades:

  - Del sistema informático de archivo de datos: no todos los computadores tienen clave de acceso, no todos los computadores que tienen clave de acceso tienen configuradas claves fuertes de acceso al computador como tal y al programa contable QuickBooks, no todas las redes tienen

claves fuertes de accesos, no todos los computadores tienen sus licencias vigentes, no está actualizado el nivel de acceso de los diferentes usuarios a los computadores de otros usuarios en la red interna, los correos electrónicos se manejan desde Outlook y no directamente de un browser, se mantiene en archivo información de datos personales innecesaria u obsoleta, en trabajo remoto o teletrabajo los usuarios se conectan desde redes no autorizadas o inseguras, los usuarios respaldan la información de la empresa en medios no autorizados o inseguros, no está establecida y actualizada una normativa de ciberseguridad adecuada, los usuarios no cumplen a cabalidad las normas indicadas en el manual de organización en el apartado referente a equipos de computación que indica lo siguiente:

Todos los equipos de computación y el servicio de internet de la Empresa deberán ser utilizados estrictamente para la realización de las actividades laborales. Por tanto, está terminantemente prohibido el uso de esta infraestructura en actividades personales tales como:

a) Atender correos electrónicos personales, usar la cuenta de correo de la Empresa en comunicaciones no laborales, realizar pagos o compras personales en línea, revisar páginas no relacionadas con la actividad laboral.
b) Usar medios de comunicación que afecten la productividad en el trabajo tales como mensajes de texto conocidos como “chat” o “messenger” o cualquier otro medio de comunicación que no tenga que nada que ver con la gestión empresarial tales como redes sociales tipo Facebook, Hi5, MySpace, Skype u otras.
c) Instalar descargadores de música, juegos u otros programas no relacionados con la actividad laboral o descargar antivirus sin autorización escrita del Gerente General.
d) El escuchar música por YouTube o por cualquier otro medio que consuma el ancho de banda del internet de la Empresa restándole velocidad y, por ende, eficiencia.
e) El usar el Wifi de la Empresa sin autorización del Gerente General. Este servicio solo aplica para visitantes y emergencias laborales en las que la red de internet de la Empresa no funcione.
f) En general está prohibido el uso indebido del software, incluidos archivos electrónicos y programas contables, así como del hardware, incluidas las impresoras. Estos recursos no deben ser usados en actividades personales tales como elaboración y/o impresión de deberes académicos propios o de sus hijos.

Además, es obligación de cada usuario apagar correctamente el CPU, monitor, impresora, UPS y desconectar el UPS como tal o el cortapicos o el protector de voltaje del tomacorriente respectivo para prevenir daños en los equipos de computación o de cualquier otro equipo sensible o costoso ocasionado por variaciones de voltaje o tormentas eléctricas.

Esta disposición tiene alcance para la maquinaria y equipos de fábrica y laboratorio. Por tanto, es importante que el usuario de cada equipo se asegure de que éste cuente con el respectivo equipo de protección eléctrica, según lo requerido por cada proveedor.

Por tanto, se debe documentar a más de los manuales de operación de los equipos, cuáles son los requerimientos adicionales para ponerlos en marcha y protegerlos, particulares que deben ser socializados de manera evidenciable con los usuarios respectivos.

Se hace hincapié en el apagado y desconexión del UPS puesto que, a más de los riesgos indicados, si se va la energía eléctrica por largo tiempo la batería del UPS se agotará y deberá ser repuesta. En caso de que esto suceda, el usuario del equipo deberá asumir el costo de reposición de la batería.

Por otro lado, es responsabilidad de cada colaborador el respaldar su información laboral de manera continua, esto es por lo menos una vez cada mes, para evitar grandes pérdidas de información laboral en caso de averías severas o robo de los equipos de computación.

En caso de pérdida de información por falta de precaución, el tiempo dedicado a su recuperación y/o re-elaboración tendrá que ser realizado fuera de la jornada laboral sin derecho a remuneración alguna.

Se recomienda especial cuidado en el uso de los medios de almacenamiento externos tales como flash memory que han sido utilizadas por el personal en lugares públicos o son de propiedad de terceros, por el riesgo de infección y contagio de virus que pueden generar en la red de la Empresa.

También se recomienda tener flash memory exclusivas para compartir información solo dentro de la red de la Empresa. De igual manera, se recomienda correr el antivirus a los medios de almacenamiento que pudieran contener información infectada, aunque ningún antivirus es 100% seguro.

En caso de que un equipo de trabajo se encuentre infectado por la inobservancia comprobada a esta recomendación o por abrir páginas o correos riesgosos, el arreglo del equipo correrá a cargo del colaborador que infringió en esta norma y será sancionado de acuerdo a la gravedad de la falta.

La Empresa se reserva el derecho de revisar en cualquier momento los archivos de los equipos de computación y de todos los correos electrónicos usados desde la cuenta asignada a cada usuario por la Empresa. De igual manera, la Empresa se reserva el derecho de colocar los bloqueos y seguridades que considere pertinentes para garantizar el uso apropiado de los equipos en mención.

En caso de existir alguna anomalía causada por un colaborador en la información electrónica empresarial que afecte a la productividad de la misma, éste será responsable de los daños y perjuicios ocasionados y del lucro cesante derivado de su falta, si lo hubiere.

Toda la información contenida en los computadores o en cualquier otro medio externo de almacenamiento es considerada como de carácter confidencial y de propiedad de la Empresa. Esto incluye el acceso y visualización de las cámaras de vigilancia las cuales solo podrán ser utilizadas por el personal autorizado dentro de las instalaciones de la Empresa.

La colocación de claves de acceso a los computadores será obligatoria solo para las Jefaturas u otros puestos que manejan información confidencial relevante. Las claves de acceso a los computadores y a páginas web de índole laboral deberán ser informadas al Gerente General cada vez que sean requeridas o cambiadas.

El Gerente General será el responsable de autorizar la dotación, renovación y mantenimiento de los equipos de computación, redes, internet u otros servicios relacionados. Por tanto, el personal deberá comunicar por escrito cualquier anomalía detectada para que el Gerente General direccione la solución al problema de manera directa con el proveedor o a través del mismo usuario.

Finalmente, se recomienda enviar los correos electrónicos solo al personal relacionado con el tema tratado para evitar pérdidas de tiempo de los colaboradores que no tienen necesidad de enterarse de lo que no les compete.

El uso incorrecto o la falta de cuidado en el manejo de los equipos de computación o de la información que éstos contienen serán considerados como faltas extremadamente graves que darán lugar a una causal para solicitar el visto bueno.

- Del sistema físico de archivo de datos: el mobiliario en donde está archivada la información física carece de llave o no se cierra con llave, se mantiene en archivo información de datos personales innecesaria u obsoleta, los usuarios de los datos personales extravían la información de los clientes, se entrega información de datos personales a los usuarios sin control por parte de los custodios, los registros que utilizan los usuarios de datos personales contienen información innecesaria en extensión y cantidad, los lugares en donde se guardan los archivos físicos no tienen las suficientes protecciones en relación a la prevención de un incendio o un robo.

2) Determinar las medidas de seguridad aplicables.

Medidas de seguridad aplicables al riesgo medio de que la amenaza causada por un ataque informático ocurra:

- Claves: verificar que el 100% de los usuarios de los computadores de la empresa configuren una clave fuerte de acceso a su computador y correos electrónicos, esto es, claves de mínimo ocho caracteres que incluyan por lo menos una letra mayúscula, una letra minúscula, un número, un carácter especial.

  La frecuencia de cambio de claves se debe hacer cada vez que el usuario lo considere pertinente, cada vez que haya tenido que compartir su clave por alguna razón laboral con autorización de gerencia general y/o mínimo cada trimestre en la fecha establecida por el jefe de talento humano y seguridad y salud ocupacional, esto es el 26 de cada uno de los siguientes meses de cada año: marzo, junio, septiembre y diciembre.

  Cada usuario tendrá la obligación de informar la clave vigente de su computador de manera directa a gerencia general a través de un mensaje de WhatsApp el cual deberá ser borrado de cada dispositivo por parte del emisor y receptor del mensaje.

  Además, los bloqueos de pantalla de los computadores deben estar configurados máximo cada 10 minutos.

- Licencias: verificar que el 100% de los usuarios de los computadores de la empresa cuenten con las licencias vigentes y necesarias. Esto aplica para licencias de programas y antivirus adquiridos por la empresa.

- Redes de conexión a internet: el único proveedor calificado para contratar el servicio de internet de la empresa es Netlife a través de la empresa Megadatos. Solo para el caso de las islas ubicadas en centros comerciales se tendrá que contratar a un proveedor diferente conforme a lo dispuesto por cada centro comercial.

  Tanto los módems como los routers y cualquier otro dispositivo de conexión a internet deberán tener claves fuertes conforme a lo establecido en los párrafos precedentes. La contraseña de Wi-fi solo podrá ser compartida a visitantes de la empresa o a los colaboradores en caso de alguna necesidad laboral.

  Como regla general, no estará permitida la conexión remota a los computadores de la empresa. Para el caso de las excepciones, éstas se aplicarán por puestos de trabajo previa calificación de la seguridad por parte del proveedor de servicios de hardware y software de la empresa y con la debida autorización escrita por correo electrónico de gerencia general.

- Redes de conexión interna entre computadores de la empresa: verificar que estén bloqueados todos los accesos entre computadores, es decir, ningún computador podrá acceder a otro computador a través de la red de conexión física por cableado y/o red inalámbrica. En caso de tener alguna necesidad de conexión entre computadores se deberán utilizar programas tipo AnyDesk o TeamViewer.

- Plataforma de correos electrónicos: los correos de la empresa están migrando de Web Mail a Zoho Mail que ofrece una mejor protección de datos y contra amenazas.

  Conforme a lo que informa Zoho Mail en su página web, el sofisticado mecanismo de protección contra amenazas de Zoho Mail identifica y elimina las amenazas antes de que lleguen a la bandeja de entrada. Las herramientas de protección de datos resguardan la integridad de los datos frente a cualquier amenaza o pérdida. Mediante el uso de protocolos, políticas y mecanismos sistemáticos, Zoho Mail está listo para evitar la falsificación de correos electrónicos, la suplantación de identidad, el correo no deseado y la fuga de datos.

  Otra ventaja que ofrece la migración de la plataforma de correos electrónicos es que se podrá trabajar directamente en el browser de Zoho Mail sin tener la necesidad de utilizar un gestor de correo adicional tal como Outlook. Además, se contará con un mayor espacio de almacenamiento de correos en la nube de Zoho Mail conforme a lo establecido en los planes contratados.

- Servidor del sistema contable: el sistema contable que actualmente utilizada la empresa se denomina QuickBooks. La empresa calificada como proveedora de este servicio es APower la cual almacena la información de sus clientes en los servidores de Amazon.

- Políticas de uso de los equipos de computación: todo usuario autorizado de los equipos de computación de la empresa tendrá la obligación de cumplir con las siguientes políticas:

3) Verificar, evaluar y valorar continua y permanentemente la eficiencia, eficacia y efectividad de las medidas de seguridad aplicables (de carácter técnico, organizativo o de cualquier otra índole) con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales, y evidenciar que mitigan de forma adecuada los riesgos identificados.

4) Notificar la vulneración de seguridad.