JAPDEVA

AUDITORÍA GENERAL

INFORME No. AG-AR-002-18

(02-07-2018)

EVALUACIÓN DE INTERNET Y CORREO ELECTRÓNICO EN JAPDEVA, SEGÚN LEY 8968 (PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE DATOS PERSONALES) Y EL USO DE EQUIPO INSTITUCIONAL

JULIO, 2018

EVALUACIÓN DE INTERNET Y CORREO ELECTRÓNICO EN JAPDEVA, SEGÚN LEY 8968 (PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE DATOS PERSONALES) Y EL USO DEL EQUIPO INSTITUCIONAL

ÍNDICE

Limón, 02 de julio del 2018
AG-AR-002-18

RESUMEN EJECUTIVO DEL INFORME DE AUDITORÍA

EVALUACIÓN DE INTERNET Y CORREO ELECTRÓNICO EN JAPDEVA, SEGÚN LEY 8968 (PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE DATOS PERSONALES) Y EL USO DEL EQUIPO INSTITUCIONAL

¿Qué examinamos?

La auditoría abarcó las acciones realizadas desde el 01 de enero del 2017 al 30 de mayo del 2018, ampliándose en aquellos casos en que se consideró necesario.

¿Por qué es importante?

La Institución proporciona acceso a Internet y correo electrónico a los funcionarios autorizados por sus jefaturas durante el horario laboral, para su información y comunicación, además de facilitarles el equipo informático necesario para su utilización. Sin embargo, dicho uso debe estar regulado por la normativa correspondiente, de forma tal que sea acorde con el ordenamiento jurídico y no riña con las normas comunes de la ética y buena conducta, normalmente reconocidas para la sociedad, aparte de que la navegación en Internet, uso del correo y los equipos quedan limitados única y exclusivamente para fines propios de JAPDEVA.

¿Qué encontramos?

1. Existe incongruencia entre lo regulado por el Reglamento para la utilización de recursos informáticos y el Acuerdo No. 271-10 del Consejo de Administración en cuanto al uso de chats en Internet.

2. El Departamento de Informática carece de un procedimiento formalmente establecido para el mantenimiento y puesta en producción del software e infraestructura tecnológica.

3. No se ha regulado en forma efectiva el envío de correos masivos por parte de funcionarios no autorizados.

4. El Departamento de Informática permitió el acceso al correo institucional mediante dispositivos móviles sin haber comunicado antes a los usuarios los riesgos y las medidas de seguridad a tomar.

5. La red inalámbrica de la Sala de Abordaje de Cruceros, concebida para el uso exclusivo de turistas que llegan en cruceros a Limón, es utilizada por funcionarios no autorizados y personas ajenas a la Institución.

6. El Departamento de Informática no firmó Acuerdos de Servicios o Contratos de Confidencialidad con las últimas dos empresas contratadas.

7. No hay certeza de que el proyecto de implementación del correo "en la nube" cumpla con lo establecido en la Ley No. 8968 y su Reglamento en cuanto al tratamiento de datos personales.

¿Qué sigue?

1. Se recomienda a la División Financiera Contable instruir al Departamento de Informática para que actualice en los próximos tres meses el Reglamento para la utilización de recursos informáticos en forma integral y de acuerdo con los avances tecnológicos, añadiendo los puntos del Acuerdo No. 271-10 del Consejo de Administración que no se incorporaron en el año 2010 e incluyendo aspectos solicitados en informes Au-Inf-002-15, Au-Inf-006-15, Au-Inf-016-15 y AG-AR-008-17 por esta Auditoría, para su posterior publicación en el diario oficial La Gaceta, una vez que los cambios hayan sido aprobados por dicho Consejo.

2. Se insta a la División Financiera Contable a instruir al Departamento de Informática para que elabore y presente a esa División el procedimiento para el mantenimiento y puesta en producción del software e infraestructura tecnológica y las políticas relativas a la contratación de productos de software e infraestructura y para la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI, solicitados en informes anteriores de esta Auditoría.

3. Se recomienda a la División Financiera Contable instruir al Departamento de Informática en cuanto a establecer en el software Microsoft Outlook un límite máximo razonable de contactos (se sugiere 25) que el funcionario pueda seleccionar en un solo mensaje, con el fin de evitar el envío masivo de correos.

4. Se insta a la División Financiera Contable a instruir al Departamento de Informática para que informe a los usuarios del correo institucional "en la nube" los riesgos existentes y la implementación de medidas de seguridad en sus dispositivos móviles, a fin de fortalecer la confidencialidad, integridad y disponibilidad de la información.

5. Se recomienda a la División Financiera Contable instruir al Departamento de Informática para que cambie la contraseña de acceso a la red inalámbrica de la Sala de Abordaje de Cruceros y advierta en forma escrita a la jefatura y

funcionarios de la Unidad de Cruceros que dicha red es de uso exclusivo de los turistas y que a partir de ese momento son los únicos responsables de su administración, en el entendido de que no debe ser comunicada a ningún funcionario ni persona externa y en caso de que algún turista así lo requiera, se le digite en su dispositivo móvil. Una vez que el crucero zarpe, deberá inhabilitar dicha red hasta que arribe un nueva nave turística.

6. Se insta a la División Financiera Contable a instruir al Departamento de Informática para que desarrolle e implemente un mecanismo de acceso más ágil y efectivo a la red inalámbrica de la Sala de Abordaje de Cruceros, como por ejemplo el utilizado en puertos y aeropuertos de otros países, el cual permite al turista identificarse en Internet y utilizarla solo un día en el mes, por un periodo de tiempo limitado (30 o 60 minutos).

7. Se recomienda a la División Financiera Contable instruir al Departamento de Informática para que firme Acuerdos de Servicios, Contratos de Confidencialidad o ambos documentos con las empresas contratadas, según corresponda, cuando se desarrollen e implementen proyectos de hardware, software e infraestructura tecnológica.

8. Se insta a la División Financiera Contable a instruir al Departamento de Informática para que firme Acuerdos de Confidencialidad con las empresas contratadas, acordes con la Ley No. 8968 y su Reglamento, en caso de que los proyectos a desarrollar e implementar involucren el tratamiento de datos personales y/o sensibles de los funcionarios, incluyendo la posibilidad de iniciar esta tarea con la firma SOFTWAREONE COSTA RICA S. A., quien se encargó de implementar el correo electrónico "en la nube".

INFORME DE AUDITORÍA No. AG-AR-XXX-18

EVALUACIÓN DE INTERNET Y CORREO ELECTRÓNICO EN JAPDEVA, SEGÚN LEY 8968 (PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE DATOS PERSONALES) Y EL USO DEL EQUIPO INSTITUCIONAL

1. INTRODUCCIÓN.

1.1 ORIGEN DEL ESTUDIO.

La presente evaluación de Internet y correo electrónico en JAPDEVA, según Ley 8968 (Protección de la persona frente al tratamiento de datos personales) y el uso de equipo institucional, forma parte del Plan Anual de Trabajo de la Auditoría General para el año 2018.

1.2 OBJETIVOS DEL ESTUDIO.

1.2.1 OBJETIVO GENERAL.

Evaluar la existencia de normativa que regule el uso de Internet y correo electrónico en horas laborales, tanto institucional como personal.

1.2.2 OBJETIVOS ESPECÍFICOS.

- Determinar si está normado el uso de correo electrónico e Internet en las oficinas institucionales.
- Validar si se cumple con la normativa vigente para el uso y acceso a Internet y correo electrónico.
- Indicar las medidas correctivas que permitan contar con lineamientos para el control y uso racional de redes informáticas por parte del personal.

1.3 EQUIPO DE TRABAJO.

- Marvin Jiménez León, Auditor General.
- Mainor Segura Bejarano, Sub-Auditor General.
- Néstor Anderson Salomons, Supervisor de Auditoría.
- Mainor Loría Núñez, Auditor Designado.

1.4 ALCANCE DEL ESTUDIO Y PERÍODO REVISADO.

El estudio abarcó procedimientos, actividades y documentación sobre el uso de Internet, correo electrónico y equipo institucional, mediante el análisis de la información relacionada, según se detalla:

- Normas para el uso de Internet, correo electrónico y equipo institucional, definidas en el Reglamento para la utilización de recursos informáticos (publicado en La Gaceta No. 6 del 09 de enero del 2006).
- Normas para el uso de Internet, correo electrónico y equipo institucional, definidas en los Acuerdos del Consejo de Administración No. 37-2002 y No. 271-10.

Adicionalmente se efectuaron entrevistas a los siguientes funcionarios, relacionados ambos con la materia.

- Ing. Rafael Rivas Delgado, Jefe Departamento de Informática.
- Licda. María Luz Acosta Gómez, Jefa Sección de Soporte Técnico.

Para la ejecución del trabajo se observaron las políticas definidas en el Manual de Normas Generales de Auditoría para el Sector Público (R-DC-064-2014), Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE), Directrices Generales sobre Principios y Enunciados Éticos a observar por parte de los jerarcas, titulares subordinados, funcionarios de la CGR, auditorías internas y servidores públicos en general (D-2-2004-CO). Asimismo, se observó lo estipulado en la siguiente normativa:

- Ley General de Control Interno No. 8292.
- Ley No. 8968 (Protección de la persona frente al tratamiento de sus datos personales).
- Reglamento a la Ley No. 8968.
- Normas Técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE).
- Reglamento para la utilización de recursos informáticos (publicado en La Gaceta No. 6 del 09 de enero del 2006).

El período que abarca el estudio está comprendido entre el 01 de enero del 2017 y el 30 de mayo del 2018, ampliándose en aquellos casos en que se consideró necesario.

1.5 LIMITACIONES.

No se presentaron limitaciones que afectaran la ejecución de la presente revisión.

2. RESULTADOS.

De la revisión efectuada se obtuvieron los siguientes resultados:

2.1 Incongruencia entre lo reglamentado y acordado en cuanto al uso de chats en Internet.

Esta Auditoría determinó que inicialmente las normas sobre el uso de microcomputadoras portátiles se establecieron mediante Acuerdo No. 612-02 del Consejo de Administración (Artículo III-e de la Sesión Ordinaria No. 37-2002, celebrada el 26 de setiembre del 2002), las cuales se incluyeron posteriormente en el capítulo V (Normas para la utilización de las microcomputadoras) del Reglamento para la utilización de recursos informáticos, publicado en La Gaceta No. 6 del 09 de enero del 2006.

Por su parte, el uso de correo electrónico e Internet se estableció en los capítulos VI (Normas para la utilización del correo electrónico y VII (Del uso de Internet) del Reglamento arriba indicado y posteriormente fueron aprobados mediante Acuerdo No. 271-10 del Consejo de Administración (Artículo III-a de la Sesión Ordinaria No. 22-2010, celebrada el 01 de julio del 2010), por recomendación expresa de la jefatura del Departamento de Informática a la Gerencia General, tal como consta en oficio GG-CT-215-10 del 19 de mayo del 2010.

En este momento lo aprobado en los artículos 8 y 9 presenta incongruencia o ambigüedad no solamente con lo formalmente establecido vía Reglamento en el año 2006, sino entre ellos, tal como se muestra a continuación:

> Artículo 8: *"la 'navegación' en Internet queda limitada única y exclusivamente para fines propios de JAPDEVA, los cuales están referidos a:*
>
> *(...)*
>
> *d. Acceso a redes sociales como (Facebook, Twitter, Skype, entre otros)".*
>
> Artículo 9: *"es absolutamente prohibido:*
>
> *a. El uso de chats".*

Al respecto, es necesario indicar que según el Diccionario de la Real Academia Española, se define como charla (**chat** en idioma inglés) como "*el intercambio de mensajes electrónicos a través de Internet, que permite establecer una conversación entre dos o varias personas*" o "*Servicio que permite mantener conversaciones mediante chats*".

El Reglamento para la utilización de recursos informáticos en su capítulo VII (Del uso de Internet), artículo 48, en lo que nos interesa, determina lo siguiente:

> "*Es absolutamente prohibido el uso de chats*" (el subrayado no es del original).

Consultado al respecto el jefe del Departamento de Informática indicó que ignora las causas de tal incongruencia o ambigüedad, ya que la publicación del Reglamento para la utilización de recursos informáticos y el Acuerdo No. 271-10 se dio cuando no se encontraba laborando en la Institución.

La incongruencia entre lo publicado en el Reglamento para la utilización de recursos informáticos y el Acuerdo No. 271-10 causa confusión en los funcionarios en cuanto al permiso o prohibición de utilizar las redes sociales para chatear, aspecto que de todas formas no puede ser controlado por el Departamento de Informática, una vez que el usuario ingresa con su usuario y contraseña a cualquiera de ellas.

2.2 Carencia de un procedimiento formal para el mantenimiento y puesta en producción de software e infraestructura.

Esta Auditoría determinó que el Departamento de Informática carece de un procedimiento formalmente establecido para el mantenimiento y puesta en producción del software e infraestructura tecnológica y de políticas relativas a la contratación de productos de software e infraestructura tecnológica y para la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI, necesarios para regular la contratación e implementación de nuevo software, como es el caso de los dos últimos sistemas adquiridos (herramienta de seguridad de Internet denominada WatchGuard e implementación del correo institucional "en la nube").

En el Glosario de las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE), publicadas por la CGR en el año 2007, se definen los siguientes conceptos:

> **Hardware**: *"todos los componentes electrónicos, eléctricos y mecánicos que integran una computadora, en oposición a los programas que se escriben para ella y la controlan (software)".*
>
> **Software**: *"los programas y documentación que los soporta que permiten y que facilitan el uso de la computadora; el software controla la operación del hardware".*

Infraestructura tecnológica: *"conjunto de componentes de hardware e instalaciones en los que se soportan los sistemas de información de la organización".*

Tecnologías de información (TI): *"conjunto de tecnologías dedicadas al manejo de la información organizacional. Término genérico que incluye los recursos de: información, software, infraestructura y personas relacionadas".*

Tal como se indicó en Informe de Auditoría No. Au-Inf-002-15 del 14 de agosto del 2015, "*el procedimiento establecido para el mantenimiento y puesta en producción del software e infraestructura tecnológica, que contiene una explicación del proceso de reporte de incidencias y del reporte de nuevos requerimientos, es informal y no establece un 'punto de retorno', o sea no considera las condiciones de regreso a la versión anterior del programa o sistema en caso de que las nuevas opciones o modificaciones a los mismos no sean satisfactorias ni incluye alguna sección relacionada con puesta en producción de hardware o instalaciones*".

Posteriormente, en Informe de Auditoría No. AG-EE-04-16 del 16 de mayo del 2016, se reiteró al Departamento de Informática la recomendación de "*elaborar y someter a la aprobación de la División Financiera Contable un procedimiento para el mantenimiento y puesta en producción del software e infraestructura tecnológica, así como los formularios para el Reporte de Incidencias y Solicitud de Nuevos Requerimientos*" y se recomendó elaborar y someter a la aprobación de las jefaturas las políticas relativas a la contratación de productos de software e infraestructura y para la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) en su capítulo I (Normas de aplicación general), artículo 1.4.6 (Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica), inciso b, en lo que nos interesa, determinan lo siguiente:

"La organización debe mantener la integridad de los procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o pérdida de información.

Para ello debe:

(...)

b) Contar con procedimientos claramente definidos para el mantenimiento y puesta en producción del software e infraestructura".

Esas mismas normas, en su capítulo III (Implementación de tecnologías de información), artículo 3.1 (Consideraciones generales de la implementación de TI), inciso a, establecen lo siguiente:

> *"La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica. Para esa implementación y mantenimiento debe:*
>
> *a) Adoptar políticas sobre la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI".*

Finalmente, en su artículo 3.4 (Contratación de terceros para la implementación y mantenimiento de software e infraestructura), incisos b, d y e de ese mismo capítulo, las Normas arriba indicadas, en lo que nos interesa, determinan lo siguiente:

> *"La organización debe obtener satisfactoriamente el objeto contratado a terceros en procesos de implementación o mantenimiento de software e infraestructura. Para lo anterior, debe:*
>
> *(...)*
>
> *b. Establecer una política relativa a la contratación de productos de software e infraestructura.*
>
> *(...)*
>
> *d. Establecer un procedimiento o guía para la definición de los "términos de referencia" que incluyan las especificaciones y requisitos o condiciones requeridas o aplicables, así como para la evaluación de ofertas.*
>
> *e. Establecer, verificar y aprobar formalmente los criterios, términos y conjunto de pruebas de aceptación de lo contratado; sean instalaciones, hardware o software".*

En oficio No. DCI-118-2017 del 22 de junio del 2017, casi dos años después de emitido el Informe No. Au-Inf-002-15, la jefatura del Departamento de Informática comunicó a esta Auditoría que "aún no se iniciado la elaboración del procedimiento y políticas arriba indicados", por lo que mediante correo electrónico del 03 de abril del 2018 se solicitó el avance en la elaboración de los documentos respectivos, sin que a la fecha de presentación del presente informe hayan sido recibidos.

La carencia de un procedimiento formalmente establecido para el mantenimiento y puesta en producción del software e infraestructura tecnológica no permite definir adecuadamente la planeación, coordinación, monitoreo y comunicación de los cambios que afectan a los recursos tecnológicos y sistemas de información, para minimizar el impacto en el ambiente de producción y en los compromisos de niveles de servicio.

Por su parte la inexistencia de políticas formalmente establecidas para la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI y la contratación de productos de software e infraestructura limita no solamente ejecutar en forma ordenada y debidamente autorizada la implementación y mantenimiento de TI, sino que dificulta obtener satisfactoriamente el objeto contratado a terceros en procesos de implementación o mantenimiento de software e infraestructura.

2.3 No se ha regulado en forma efectiva el envío de correos masivos por parte de funcionarios no autorizados.

Es necesario destacar que para administrar el correo electrónico la Institución utiliza el software Exchange Server de la empresa norteamericana Microsoft Corporation, sistema de mensajería que incluye un servidor de correo y aplicaciones de trabajo en grupo y que trabaja en conjunto con el sistema Microsoft Outlook para aprovechar las características de colaboración del mismo, tales como la capacidad para compartir calendarios y listas de contactos.

En los últimos años se dieron problemas significativos con la limitación de espacio en disco del servidor, sitio donde se almacenan los correos; en ese entonces los funcionarios no limpiaban sus correos y cuando el disco se llenaba, impedía que todos los usuarios del mismo pudieran recibir o enviar mensajes hasta que se solucionara el problema, generando un descontento por la interrupción de los servicios.

Dado lo anterior, el Departamento de Informática decidió implementar el servicio de correo institucional "en la nube", contratando dichos servicios a la empresa SOFTWAREONE COSTA RICA S. A., que permitió no solo terminar con el problema de interrupción de servicios del correo, ya que si un usuario llena su buzón de correo, no impide que los demás usuarios puedan enviar y recibir mensajes, sino utilizar las bondades del Office 365, que es un plataforma que permite acceder a documentos, calendarios, colaboradores y correos desde cualquier lugar y con cualquier dispositivo, sin necesidad de estar conectado a la red de JAPDEVA.

Según Wikipedia (La enciclopedia libre), se denomina computación "en la nube" (**cloud computing** en idioma inglés) "*a un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet. Generalmente son servidores encargados de atender las peticiones en cualquier momento; se puede tener acceso a su información o servicio, mediante una conexión a Internet desde cualquier dispositivo móvil o fijo ubicado en cualquier lugar; sirven a sus usuarios desde varios proveedores de alojamiento repartidos frecuentemente por todo el mundo*".

Sin embargo, hace aproximadamente dos años todavía el software utilizado en JAPDEVA permitía el envío de correos masivos a funcionarios no autorizados, a pesar de que tal acción está absolutamente prohibida desde el año 2006 en el Reglamento para la utilización de recursos informáticos; esa mala práctica era realizada generalmente para ensalzar las virtudes o felicitar a alguien que se pensionaba, fallecía o por algunos ex-empleados para despedirse de sus compañeros.

Según el Jefe del Departamento de Informática, en la actualidad solo se permite el envío de correos masivos a la dirección de correo grupal denominada "Todos-Japdeva" a funcionarios debidamente autorizados por sus jefaturas, pero no se ha limitado a los demás usuarios la cantidad de destinatarios que pueden seleccionar en forma manual, por lo que es posible enviar un correo masivo a un número elevado de contactos, sin estar autorizado, situación que fue debidamente corroborada por esta Auditoría el 04 de abril del 2018 al seleccionar y enviar sendos correos de prueba 95 funcionarios y luego a 125 empleados más.

El Reglamento para la utilización de recursos informáticos en su capítulo VI (Normas para la utilización del correo electrónico), artículo 45, determina lo siguiente:

> "*Queda absolutamente prohibido el envío de cadenas de correo o envío masivo de correos, excepto que estos últimos estén justificados y relacionados con las labores de los funcionarios*".

Es necesario indicar que toda la población institucional conoce la prohibición del envío de correos masivos mediante la plataforma de Microsoft Outlook, ya que es regulada por el Reglamento arriba indicado, pero a pesar de que la jefatura del Departamento de Informática comunicó el 25 de abril del 2018 que en años anteriores se notificó a los usuarios sobre dicha prohibición, inclusive mencionándoles los artículos del Reglamento que estaban infringiendo, no conserva los mensajes ni fue posible para esta Auditoría localizar los correos de recordatorio de tal infracción.

El hecho de que las jefaturas de las dependencias no realizaran recordatorios o llamadas de atención sobre la prohibición de no enviar correos masivos en años recientes, causó que se enviaran mensajes grupales injustificados o no relacionados con las labores de los funcionarios y, al no existir un límite razonable del número de contactos que pueden seleccionarse en forma manual al enviar un mensaje, es posible que los usuarios utilicen esa carencia de controles para enviar mensajes masivos y/o no autorizados, como efectivamente ocurría hace aproximadamente dos años y sucedió de nuevo el 08 de marzo del 2018, cuando la jefa de la Sección de Soporte Técnico envió un correo grupal a una cantidad considerable de contactos, sin la debida autorización de la jefatura arriba indicada.

2.4 Riesgos potenciales en el acceso al correo institucional mediante dispositivos móviles.

Una de las bondades de haber contratado a la empresa SOFTWAREONE COSTA RICA S. A. la implementación del correo institucional "en la nube" es que su acceso se permite a través de cualquier dispositivo móvil, como por ejemplo teléfonos celulares convencionales, teléfonos inteligentes ("smartphones"), tabletas y computadoras portátiles, prácticamente desde cualquier lugar del mundo que brinde acceso a Internet, situación que es desconocida para muchos funcionarios de JAPDEVA.

Sin embargo, a pesar de que el correo fue implementado en servidores externos teóricamente seguros de la empresa Microsoft Corporation, el uso de aplicaciones móviles, sin consideración de los riesgos existentes y las medidas de seguridad a tomar, podría debilitar las características de dicha seguridad (confidencialidad, integridad y disponibilidad). El eslabón más débil de la cadena es un usuario desinformado o mal capacitado, dueño de dispositivos con tecnología obsoleta y/o desprotegidos, ya que generalmente los *ciberdelincuentes* utilizan las vulnerabilidades que la mayoría de personas tienen en esos dispositivos, incrementándose los riesgos al no poseer, entre otros, software antivirus o cortafuegos.

Según el Diccionario de la Real Academia Española, se denomina **cortafuegos** (**firewall** en idioma inglés) "*a un sistema que protege redes y terminales privadas de accesos no autorizados, especialmente durante la navegación por Internet*", mientras que Wikipedia (La enciclopedia libre) define ***ciberdelincuente*** como "*una persona que comete delitos informáticos, pues lo hace mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación y tiene por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos*".

El Reglamento para la utilización de recursos informáticos en su capítulo I (Del Departamento de Informática), artículo 1°, determina lo siguiente:

> *"El Departamento de Informática es el responsable de la administración de todo el equipo de cómputo, sus accesorios y la red en cuanto al mantenimiento preventivo y correctivo del equipo, instalación y mantenimiento de software, aplicaciones desarrolladas, configuración de equipo y ubicación. En virtud de lo anterior, será responsable de instruir a cada usuario a quien se le asigne un equipo de cómputo sobre el correcto uso y mantenimiento del mismo.*
>
> *Este Departamento es también el responsable de proporcionar asesoría y asistencia técnica a los funcionarios de JAPDEVA en materia de uso del servicio de Internet y Correo Electrónico*" (el subrayado no es del original).

Por su parte las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) en su capítulo I (Normas de aplicación general), artículo 1.4.2 (Compromiso del personal con la seguridad de la información), incisos a y b, especifican lo siguiente:

> "*El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI.*
>
> *Para ello, el jerarca, debe:*
>
> *a) Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI.*
>
> *b) Implementar mecanismos para vigilar el debido cumplimiento de dichas responsabilidades*".

De acuerdo con lo descrito en el Glosario de las Normas arriba indicadas, las tres características de seguridad de la información son **confidencialidad** ("*protección de información sensible contra divulgación no autorizada*"), **integridad** ("*precisión y suficiencia de la información, así como su validez de acuerdo con los valores y expectativas del negocio*") y **disponibilidad** ("*protección de los recursos necesarios y las capacidades asociadas; implica que se cuente con la información necesaria en el momento en que la organización la requiere*").

La jefatura del Departamento de Informática conoce las medidas de seguridad publicadas por la Contraloría General de la República y que deben tomarse para asegurar razonablemente la confidencialidad, integridad y disponibilidad de la

información, pero al implementar dicho correo "en la nube" mediante la empresa Microsoft Corporation, omitió comunicarle antes a los usuarios los riesgos existentes y las medidas de seguridad a tomar, pues considera que al ser una nube privada (servicios informáticos que se ofrecen a través de Internet o de una red interna privada solo a algunos usuarios y no al público en general), con un servidor en Estados Unidos y que se replica en otros servidores, con altas medidas de seguridad, tal acción no era necesaria.

El uso de la cuenta del correo institucional en un dispositivo móvil incrementa la posibilidad de que ocurran las siguientes situaciones:

- Pérdida o robo del dispositivo, al ser un aparato más pequeño, ligero y/o caro y de la información sensible, enviada o recibida mediante correo electrónico.

- Robo de credenciales (descuido y uso de dispositivos fuera de la oficina, aparatos sin clave de acceso o bloqueo, contraseñas fáciles de adivinar o utilización negligente de las mismas, uso de claves de ingreso al correo "memorizadas" por el dispositivo).

- Conexión a redes inseguras (uso de redes inalámbricas en zonas públicas como restaurantes, aeropuertos, centros comerciales o cafés Internet; actualmente los *ciberdelincuentes* crean redes públicas con el objetivo de apoderarse o modificar información en forma no autorizada).

- La instalación de aplicaciones personales que podrían comprometer la confidencialidad de la información de JAPDEVA, riesgos derivados de coexistir en un mismo dispositivo aplicaciones de uso personal e institucional y existencia de opciones de geo posicionamiento (algunas aplicaciones permiten ubicar nuestra localización y eso puede implicar riesgos de seguridad para el funcionario).

2.5 Utilización no autorizada de la red inalámbrica en la Sala de Abordaje de Cruceros.

La red inalámbrica de la Sala de Abordaje de Cruceros fue concebida para el uso exclusivo de turistas que ingresan a Limón en cruceros, pero su contraseña ha sido manejada en forma inadecuada por la funcionaria encargada de la misma, que debería digitarla en el dispositivo de cada turista cuando así lo solicite, al menos mientras el Departamento de Informática diseña un mecanismo de acceso más ágil y efectivo.

Esta Auditoría determinó que antes de la ejecución del presente estudio dicha contraseña se pegaba en la pared y era de dominio público, pues la utilizaban funcionarios no autorizados del Edificio Multiusos y guardas del Puesto 1, así como muchas personas ajenas a JAPDEVA, entre ellas artesanos, vendedores,

estudiantes, transportistas privados y taxistas que ofrecen sus tours en el patio o fuera de las instalaciones en sus computadoras portátiles, tabletas y teléfonos celulares, tanto dentro como fuera de las instalaciones.

Durante la ejecución del presente estudio se efectuaron pruebas de acceso cuando arribaron turistas y la respuesta de la red por tanto usuario conectado es lenta, pues esos accesos concurrentes saturan el ancho de banda, lo que ocasiona un lógico malestar y quejas de dichos turistas.

Además, aunque la jefatura del Departamento de Informática comunicó a esta Auditoría que la red de cruceros es una red privada virtual (VPN) independiente de la red institucional y permite crear un túnel virtual razonablemente seguro en Internet hacia otra red o dispositivo, es vulnerable a los ataques e intrusiones de los *ciberdelincuentes,* si no se toman las medidas de seguridad adecuadas.

Si bien es cierto el manejo inadecuado del acceso a la red arriba indicada no es responsabilidad del Departamento de Informática, sí lo es el bloqueo de dicha red cuando no hay cruceros, así como prevenir a la jefatura de la Unidad de Cruceros y responsabilizar a los dos funcionarios que allí laboran, una vez que se cambie de nuevo el password, para que no lo divulguen y lo digiten en el dispositivo de cada turista que así lo requiera, al menos mientras dicho departamento diseña un mecanismo de acceso más ágil y efectivo.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) en su capítulo I (Normas de aplicación general), artículo 1.4.2 (Compromiso del personal con la seguridad de la información), incisos a y b, especifican lo siguiente:

> "*El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI.*
>
> *Para ello, el jerarca, debe:*
>
> *a) Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI.*
>
> *b) Implementar mecanismos para vigilar el debido cumplimiento de dichas responsabilidades*".

Por su parte el Reglamento para la utilización de recursos informáticos en su capítulo I (Del Departamento de Informática), artículo 1°, determina lo siguiente:

> "*El Departamento de Informática es el responsable de la administración de todo el equipo de cómputo, sus accesorios y la red en cuanto al mantenimiento preventivo y correctivo del equipo, instalación y mantenimiento de software, aplicaciones desarrolladas, configuración de equipo y ubicación. En virtud de lo anterior, será responsable de instruir a cada usuario a quien se le asigne un equipo de cómputo sobre el correcto uso y mantenimiento del mismo.*
>
> *Este Departamento es también el responsable de proporcionar asesoría y asistencia técnica a los funcionarios de JAPDEVA en materia de uso del servicio de Internet y Correo Electrónico*" (el subrayado no es del original).

Las jefaturas del Departamento de Informática y Sección de Soporte Técnico conocían que la red inalámbrica de la Sala de Abordaje de Cruceros era utilizada por funcionarios de edificios aledaños y personas externas a la Institución, pero antes de la ejecución del presente estudio omitieron indicar a los funcionarios de la Unidad de Cruceros que no debían pegar la contraseña de acceso a la red en ningún lugar ni hacerla de conocimiento de los demás funcionarios y/o personas externas, pues una de sus responsabilidades es precisamente la asesoría y asistencia técnica a los funcionarios de JAPDEVA en el uso de Internet.

El hecho de permitir el acceso a la red inalámbrica de la Sala de Abordaje de Cruceros a funcionarios no autorizados y a una cantidad considerable de personas ajenas a la Institución no solamente afecta negativamente el tiempo de respuesta de la misma, sino que podría permitir una posible intrusión o daños de *ciberdelincuentes* a los recursos institucionales de TI (aplicaciones, información e infraestructura tecnológica).

2.6 No se firmaron Acuerdos de Servicios y/o Contratos de Confidencialidad con las últimas dos empresas contratadas.

Esta Auditoría determinó que el Departamento de Informática no firmó Acuerdos de Servicios o Contratos de Confidencialidad con las empresas SOFTWAREONE COSTA RICA S. A. y SYSTENET SOLUTIONS S. A., contratadas para implementar el correo institucional "en la nube" y la herramienta WatchGuard para seguridad en Internet, respectivamente.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE), en su capítulo I (Normas de aplicación general), artículo 1.4 (Gestión de la seguridad de la información), en lo que nos interesa, determina lo siguiente:

> *"La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales.*
>
> *(...)*
>
> *Además debe establecer las medidas de seguridad relacionadas con:*
>
> *El acceso a la información por parte de terceros y la contratación de servicios prestados por éstos".*

Esas mismas Normas, en el capítulo I (Normas de aplicación general), artículo 1.4.2 (Compromiso del personal con la seguridad de la información), inciso c, determinan lo siguiente:

> *"El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI.*
>
> *Para ello, el jerarca, debe:*
>
> *(...)*
>
> *c) Establecer, cuando corresponda, acuerdos de confidencialidad y medidas de seguridad específicas relacionadas con el manejo de la documentación y rescisión de contratos".*

Finalmente, las supra indicadas Normas, en su capítulo IV (Prestación de servicios y mantenimiento), artículo 4.1 (Definición y administración de acuerdos de servicio), establecen lo siguiente:

> *"La organización debe tener claridad respecto de los servicios que requiere y sus atributos, y los prestados por la Función de TI según sus capacidades.*
>
> *El jerarca y la Función de TI deben acordar los servicios requeridos, los ofrecidos y sus atributos, lo cual deben documentar y considerar como un criterio de evaluación del desempeño. Para ello deben:*

a) Tener una comprensión común sobre: exactitud, oportunidad, confidencialidad, autenticidad, integridad y disponibilidad.

b) Contar con una determinación clara y completa de los servicios y sus atributos, y analizar su costo y beneficio.

c) Definir con claridad las responsabilidades de las partes y su sujeción a las condiciones establecidas.

d) Establecer los procedimientos para la formalización de los acuerdos y la incorporación de cambios en ellos.

e) Definir los criterios de evaluación sobre el cumplimiento de los acuerdos.

f) Revisar periódicamente los acuerdos de servicio, incluidos los contratos con terceros".

Según lo establecido en el Glosario de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, se define **Acuerdo de Confidencialidad** como *"un convenio suscrito entre la entidad y sus funcionarios, o bien, entre instituciones que comparten datos o sistemas, para garantizar el manejo discreto de la información. También se utiliza el concepto 'cláusulas de confidencialidad', que son aquellas que imponen una obligación negativa: de no hacer o de abstenerse; es decir, de no utilizar la información recibida con fines distintos a los estipulados (véase el artículo 71 del Código de Trabajo)".*

Ese mismo Glosario establece que los **Acuerdos de Servicios**, mejor conocidos como convenios o acuerdos de nivel de servicio ("SLA's" por sus siglas en inglés de "Service Level Agreement") son *"contratos escritos, formales, desarrollados conjuntamente por el proveedor del servicio de TI y los usuarios respectivos, en los que se define, en términos cuantitativos y cualitativos, el servicio que brindará la dependencia responsable de TI y las responsabilidades de la contraparte beneficiada por dichos servicios.*

En cuanto a los Acuerdos de Servicios, la organización debe tener claridad respecto de los servicios que requiere y sus atributos, y los prestados por la Función de TI según sus capacidades".

La jefatura del Departamento de Informática conoce el concepto de Acuerdos de Confidencialidad y Acuerdos de Servicios, definidos en el Glosario de las Normas arriba citadas, pero no suscribió ninguno de ellos con las empresas SOFTWAREONE COSTA RICA S. A. y SYSTENET SOLUTIONS S. A.

Al no firmarse Acuerdos de Confidencialidad y/o Acuerdos de Servicios con las empresas contratadas para implementar temas sensibles como seguridad de Internet y correo electrónico "en la nube", no es posible garantizar el manejo discreto de la información ni impedir que la información recibida sea utilizada con fines distintos a los estipulados, aparte de que resulta difícil definir con claridad las responsabilidades de las partes y su sujeción a las condiciones establecidas, una vez recibidos los proyectos por parte de los proveedores, en ausencia de dichos acuerdos.

2.7 No hay certeza de que el proyecto de implementación del correo "en la nube" cumpla con lo establecido en la Ley No. 8968 y su Reglamento.

Como se informó en el punto anterior, esta Auditoría determinó que el Departamento de Informática no firmó un Contrato de Confidencialidad con las empresa SOFTWAREONE COSTA RICA S. A., aparejado a la Ley No. 8968 (Protección de la persona frente al tratamiento de datos personales) y el Reglamento a dicha ley.

Es necesario destacar que esa Ley y su Reglamento son claros en que las empresas encargadas y/o responsables de las bases de datos (en el sitio o "en la nube") e intermediarios tecnológicos deben adoptar las medidas de índole técnica y de organización, necesarias para garantizar la seguridad y confidencialidad de los datos de carácter personal (cualquier dato relativo a una persona física identificada o identificable) y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, aparte de que están obligadas al secreto profesional, aun después de finalizada su relación con la base de datos.

La Ley No. 8968 (Protección de la persona frente al tratamiento de sus datos personales), capítulo I (Disposiciones generales), sección única, artículo 3 (Definiciones), en lo que nos interesa, determina lo siguiente:

"Para los efectos de la presente ley se define lo siguiente:

(...)

b) Datos personales: cualquier dato relativo a una persona física identificada o identificable.

(...)

e) Datos sensibles: información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones

religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros.
f) Deber de confidencialidad: obligación de los responsables de bases de datos, personal a su cargo y del personal de la Agencia de Protección de Datos de los Habitantes (Prodhab), de guardar la confidencialidad con ocasión del ejercicio de las facultades dadas por esta ley, principalmente cuando se acceda a información sobre datos personales y sensibles. Esta obligación perdurará aun después de finalizada la relación con la base de datos.

(...)

h) Responsable de la base de datos: persona física o jurídica que administre, gerencie o se encargue de la base de datos, ya sea esta una entidad pública o privada, competente, con arreglo a la ley, para decidir cuál es la finalidad de la base de datos, cuáles categorías de datos de carácter personal deberán registrase y qué tipo de tratamiento se les aplicarán.

i) Tratamiento de datos personales: cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros".

Esa misma Ley, en su sección III (Seguridad y confidencialidad del tratamiento de los datos), establece lo siguiente:

Artículo 10 (Seguridad de los datos): *"el responsable de la base de datos deberá adoptar las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a esta ley.*

Dichas medidas deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada.

No se registrarán datos personales en bases de datos que no reúnan las condiciones que garanticen plenamente su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas.

Por vía de reglamento se establecerán los requisitos y las condiciones que deban reunir las bases de datos automatizadas y manuales, y de las personas que intervengan en el acopio, almacenamiento y uso de los datos".

Artículo 11 (Deber de confidencialidad)*: "la persona responsable y quienes intervengan en cualquier fase del tratamiento de datos personales están obligadas al secreto profesional o funcional, aun después de finalizada su relación con la base de datos. La persona obligada podrá ser relevada del deber de secreto por decisión judicial en lo estrictamente necesario y dentro de la causa que conoce".*

Por su parte el Reglamento a la Ley No. 8968, capítulo I (Disposiciones generales), determina lo siguiente:

Artículo 1 (Objeto): *"las presentes disposiciones tienen por objeto reglamentar la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, en cuanto a garantizar a cualquier individuo, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su intimidad o actividad privada, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes".*

Artículo 2 (Definiciones, siglas y acrónimos).

(...)

b) "Base de datos: Cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales públicos o privados, que sean objeto de tratamiento, automatizado o manual, en el sitio o en la nube, bajo control o dirección de un responsable, cualquiera que sea la modalidad de su elaboración, organización o acceso.

c) Base de datos interna, personal o doméstica: Cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales públicos o privados, mantenidos por personas físicas o jurídicas con fines exclusivamente internos, personales o domésticos, siempre y cuando éstas no sean venidas o administradas con fines de distribución, difusión o comercialización.

(...)

e) Comercializar: Vender, transar, intercambiar o de cualquier manera enajenar o pignorar, con fines de lucro a favor de un tercero, una o más veces, aquellos datos personales que consten en bases de datos.

(…)

i) Datos en la nube: Archivo, fichero, registro u otro conjunto estructurado de datos a los cuales se accesa haciendo uso de Internet.

j) Distribución, difusión: Cualquier forma en la que se repartan o publiquen datos personales, a un tercero, por cualquier medio.

k) Encargado: Toda persona física o jurídica, entidad pública o privada, o cualquier otro organismo que da tratamiento a los datos personales por cuenta del responsable de la base de datos.

(…)

n) Intermediario tecnológico o proveedor de servicios: Persona física o jurídica, pública o privada que brinde servicios de infraestructura, plataforma, software u otros servicios, sin realizar tratamiento de datos personales.

(…)

s) Responsable: Toda persona física o jurídica, pública o privada, que administre o, gerencia o, se encargue o, sea propietario, de una o más bases de datos públicas o privadas, competente con arreglo a la Ley, para decidir cuál es la finalidad de la base de datos, cuáles categorías de datos de carácter personal deberán registrarse y qué tipo de tratamiento les aplicarán".

Artículo 3 (Ámbito de aplicación): *"este Reglamento será de aplicación a los datos personales que figuren en las bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos, en tanto surtan efectos dentro del territorio nacional, o les resulte aplicable la legislación costarricense derivada de la celebración de un contrato o en los términos del derecho internacional. El régimen de protección de los datos de carácter personal que se establece en este Reglamento, no será de aplicación a las bases de datos mantenidas por personas físicas o jurídicas, públicas o privadas, con fines exclusivamente internos, personales o domésticos, siempre y cuando éstas no sean de cualquier manera comercializadas. No será de aplicación este Reglamento a los datos referentes al comportamiento crediticio que se regirán por la normativa especial del Sistema Financiero Nacional".*

Ese mismo Reglamento, en su capítulo IV (Del Tratamiento de los Datos Personales y las Medidas de Seguridad), establece lo siguiente:

Artículo 27 (Procedimientos para el tratamiento): *"el responsable establecerá y documentará procedimientos para la inclusión, conservación, modificación, bloqueo y supresión de los datos personales, en el sitio o en la nube, con base en los protocolos mínimos de actuación y las medidas de seguridad en el tratamiento de los datos personales. Además deberá el responsable de la base de datos velar por la aplicación del principio de calidad de la información".*

Artículo 28 (Condiciones del tratamiento): *"corresponde al responsable o al encargado, la difusión, comercialización y distribución de dichos datos, según lo que determine el consentimiento informado otorgado por el titular, aún y cuando estos datos sean almacenados o alojados por un intermediario tecnológico".*

Artículo 29 (Contratación o subcontratación de servicios): *"se podrá contratar o subcontratar los servicios del intermediario tecnológico o proveedor de servicios, siempre y cuando no implique tratamiento de datos personales. El responsable deberá verificar que dicho intermediario o proveedor cumpla con las medidas de seguridad mínimas que garanticen la integridad y seguridad de los datos personales".*

Artículo 30 (Tratamiento de datos por parte del encargado): *"el encargado solo podrá intervenir en el tratamiento de las bases de datos personales, según lo establecido en el contrato celebrado con el responsable y sus indicaciones".*

Artículo 31 (Obligaciones del encargado): *"el encargado tendrá las siguientes obligaciones en el tratamiento de las bases de datos personales:*

a) Tratar únicamente los datos personales conforme a las instrucciones del responsable;

b) Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;

c) Implementar las medidas de seguridad y cumplir con los protocolos mínimos de actuación conforme a la Ley, el presente Reglamento y las demás disposiciones aplicables;

d) Guardar confidencialidad respecto de los datos personales tratados;

e) Abstenerse de transferir o difundir los datos personales, salvo instrucciones expresas por parte del responsable.

f) Suprimir los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales".

La jefatura del Departamento de Informática conoce el concepto de Acuerdo de Confidencialidad y la existencia de la Ley No. 8968 y su Reglamento, pero no suscribió acuerdo legal alguno con la empresa SOFTWAREONE COSTA RICA S. A. en cuanto al tratamiento y protección de los datos personales de los funcionarios.

Al no haberse firmado un Contrato de Confidencialidad con la empresa SOFTWAREONE COSTA RICA S. A., acorde a la Ley No. 8968 y su Reglamento, la Institución carece de un documento legal u oficial que permita controlar en forma razonable cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros.

2.8 Análisis de riesgos y mapa térmico.

En el Anexo No. 1 se presentan los riesgos más relevantes, analizados en el presente estudio, considerando su probabilidad de ocurrencia, calificación (según su impacto para la Administración activa y Auditoría), nivel del riesgo y controles asociados, establecidos por dicha administración.

3. CONCLUSIONES.

De conformidad con los resultados del presente estudio, esta Auditoría arribó a las siguientes conclusiones:

3.1 Existe incongruencia entre lo regulado por el Reglamento para la utilización de recursos informáticos y el Acuerdo No. 271-10 del Consejo de Administración en cuanto al uso de chats en Internet.

3.2 El Departamento de Informática carece de un procedimiento formalmente establecido para el mantenimiento y puesta en producción del software e infraestructura tecnológica.

3.3 No se ha regulado en forma efectiva el envío de correos masivos por parte de funcionarios no autorizados.

3.4 El Departamento de Informática permitió el acceso al correo institucional mediante dispositivos móviles sin haber comunicado antes a los usuarios los riesgos y las medidas de seguridad a tomar.

3.5 La red inalámbrica de la Sala de Abordaje de Cruceros, concebida para el uso exclusivo de turistas que llegan en cruceros a Limón, es utilizada por funcionarios no autorizados y personas ajenas a la Institución.

3.6 El Departamento de Informática no firmó Acuerdos de Servicios o Contratos de Confidencialidad con las últimas dos empresas contratadas.

3.7 No hay certeza de que el proyecto de implementación del correo "en la nube" cumpla con lo establecido en la Ley No. 8968 y su Reglamento en cuanto al tratamiento de datos personales.

4. RECOMENDACIONES.

De conformidad con los hechos señalados y las conclusiones a las que arribó, esta Auditoría se permite efectuar las siguientes recomendaciones:

Para la División Financiera Contable:

4.1 Instruir al Departamento de Informática para que actualice en los próximos tres meses el Reglamento para la utilización de recursos informáticos en forma integral y de acuerdo con los avances tecnológicos, añadiendo los puntos del Acuerdo No. 271-10 del Consejo de Administración que no se incorporaron en el año 2010 e incluyendo aspectos solicitados en informes Au-Inf-002-15, Au-Inf-006-15, Au-Inf-016-15 y AG-AR-008-17 por esta Auditoría, para su posterior publicación en el diario oficial La Gaceta, una vez que los cambios hayan sido aprobados por dicho Consejo.

4.2 Instruir al Departamento de Informática para que elabore y presente a esa División el procedimiento para el mantenimiento y puesta en producción del software e infraestructura tecnológica y las políticas relativas a la contratación de productos de software e infraestructura y para la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI, solicitados en informes anteriores de esta Auditoría.

4.3 Instruir al Departamento de Informática en cuanto a establecer en el software Microsoft Outlook un límite máximo razonable de contactos (se sugiere 25) que el funcionario pueda seleccionar en un solo mensaje, con el fin de evitar

el envío masivo de correos.

4.4 Instruir al Departamento de Informática para que informe a los usuarios del del correo institucional "en la nube" los riesgos existentes y la implementación de medidas de seguridad en sus dispositivos móviles, a fin de fortalecer la confidencialidad, integridad y disponibilidad de la información.

4.5 Instruir al Departamento de Informática para que cambie la contraseña de acceso a la red inalámbrica de la Sala de Abordaje de Cruceros y advierta en forma escrita a la jefatura y funcionarios de la Unidad de Cruceros que dicha red es de uso exclusivo de los turistas y que a partir de ese momento son los únicos responsables de su administración, en el entendido de que no debe ser comunicada a ningún funcionario ni persona externa y en caso de que algún turista así lo requiera, se le digite en su dispositivo móvil. Una vez que el crucero zarpe, deberá inhabilitar dicha red hasta que arribe una nueva nave turística.

4.6 Instruir al Departamento de Informática para que desarrolle e implemente un mecanismo de acceso más ágil y efectivo a la red inalámbrica de la Sala de Abordaje de Cruceros, como por ejemplo el utilizado en puertos y aeropuertos de otros países, el cual permite al turista identificarse en Internet y utilizarla solo un día en el mes, por un periodo de tiempo limitado (30 o 60 minutos).

4.7 Instruir al Departamento de Informática para que firme Acuerdos de Servicios, Contratos de Confidencialidad o ambos documentos con las empresas contratadas, según corresponda, cuando se desarrollen e implementen proyectos de hardware, software e infraestructura tecnológica.

4.8 Instruir al Departamento de Informática para que firme Acuerdos de Confidencialidad con las empresas contratadas, acordes con la Ley No. 8968 y su Reglamento, en caso de que los proyectos a desarrollar e implementar involucren el tratamiento de datos personales y/o sensibles de los funcionarios, incluyendo la posibilidad de iniciar esta tarea con la firma SOFTWAREONE COSTA RICA S. A., quien se encargó de implementar el correo electrónico "en la nube".

Cordialmente,

Lic. Mainor Loría Núñez
Auditor Designado

MBA Néstor Anderson Salomons
Supervisor de Auditoría

Lic. Marvin Jiménez León
Auditor General

JAPDEVA AUDITORIA GENERAL

ANEXO No. 1: Análisis de riesgos y mapa térmico

A. Posibles Riesgos o eventos	Calificación (Según su impacto para la Auditoría Interna)	Calificación (Según su impacto para la Administración activa)	Nivel de riesgo (B*C)
Implementación del correo institucional "en la nube" y uso del mismo en dispositivos móviles, sin antes informar a los usuarios las medidas de seguridad y protección necesarias	4.5	5	Muy alto
Inexistencia de un Acuerdo de Confidencialidad con el intermediario tecnológico o proveedor de servicios del correo electrónico "en la nube", aparejado a la Ley No. 8968 y su Reglamento, lo que no permite asegurar razonablemente la protección de datos personales de los usuarios	3.5	5	Muy alto
El uso público o generalizado de la red inalámbrica de la Sala de Abordaje, la cual es exclusiva para los turistas que ingresan al país en cruceros, facilita la comisión de sabotaje, intrusiones, robo o pérdida de información y hackeo de la red institucional por parte de terceros	4	5	Muy alto
Carencia de un procedimiento para el mantenimiento y puesta en producción del software e infraestructura tecnológica, lo que no permite definir adecuadamente la planeación, coordinación, monitoreo y comunicación de los cambios que afectan a los recursos tecnológicos y sistemas de información	4	4.5	Muy alto
El Acuerdo del Consejo de Administración No. 271-10 del 2010 riñe con lo dispuesto en el Reglamento para la utilización de recursos informáticos del 2006 y dos de sus artículos se contradicen, lo que podría confundir al usuario en cuanto al uso o prohibición de chats	5	4.5	Muy alto

Área de mapa Térmico	
Muy alto	5
Medio	0
Bajo	0
Muy bajo	0