**INFORME DE AUDITORÍA INTERNA AI JPS N° 19-2018**

**ÁREA SISTEMAS**

**TEMA:**

# VERIFICACIÓN Y EVALUACIÓN DE LOS PLANES DE CONTINUIDAD DE LOS SERVICIOS INFORMÁTICOS A NIVEL DE LA JUNTA DE PROTECCIÓN SOCIAL

**PREPARADO POR:**

**ANDRÉS MARTÍNEZ PORRAS**
**PROFESIONAL II**

**WEN JIE ZHEN WU**
**PROFESIONAL II**

**FECHA:**

**21 DE DICIEMBRE DE 2018**

**DIRIGIDO A:**

**DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN**

**COPIA:**

**GERENCIA GENERAL**

# INDICE DEL INFORME

# RESUMEN EJECUTIVO

## Informe de Auditoría Nº 19-2018

## Verificación y evaluación de los planes de continuidad de los servicios informáticos a nivel de la Junta de Protección Social

En cumplimiento al Plan Anual de Trabajo para el año 2018, se realizó un estudio para verificar los planes de continuidad elaborados por el Departamento de Tecnologías de Información sobre los sistemas informáticos utilizados en los procesos institucionales y las diferentes pruebas realizadas en los periodos 2017 y 2018.

El objetivo general del presente estudio es verificar los planes de continuidad elaborados por el Departamento de Tecnologías de Información sobre los sistemas informáticos utilizados en los procesos institucionales.

Para la elaboración del informe se procedió a la revisión de las recomendaciones giradas en los informes N°04-2016 **"V*erificación de la seguridad e integridad de las aplicaciones informáticas, bases de datos, conectividad y otros aspectos relacionados con la comercialización de la lotería electrónica adjudicada al consorcio gtech-boldt gaming*"** y N°23-2017 "***Consultoría técnica especializada para verificar la seguridad y planes de contingencia implementados por el departamento de tecnologías de la información en los servidores, dispositivos de red, base de datos y aplicaciones informáticas***", las cuales se encuentran pendientes de cumplimiento, dichos informes fueron elaborados mediante el proceso de contratación de auditorías externas, adjudicadas a la empresa Price Waterhouse Cooper.

De acuerdo a la documentación recolectada se logró determinar que el Departamento de Tecnologías de la Información no realiza pruebas a las estrategias de continuidad del negocio desde el año 2014, aludiendo que no contaban con los contratos de proveedores, sin embargo, en una consulta realizada al Departamento de Recursos Materiales, dichos contratos estaban en vigencia en el periodo 2015, y algunos hasta el 2017.

En las políticas definidas por el Departamento de Tecnologías de la Información, se establecen varias medidas de análisis anual, sin embargo, las mismas no pudieron ser evaluadas, ya que no fueron remitidas a la fecha de conclusión del informe.

Cabe destacar, que la Auditoría Interna en su función asesora y fiscalizadora, realiza estudios en los cuales por medio de las recomendaciones giradas en sus *"Informes de Auditoría"*, trata de proporcionar una garantía razonable de que las actuaciones

del jerarca, los titulares subordinados y todos los colaboradores de la Institución se apeguen a sanas prácticas y se ejecuten dentro del marco técnico y legal vigente, por lo que se emiten recomendaciones las cuales se dirigen a fortalecer la estructura de control interno.

Por su parte, a la Administración le corresponde valorar dentro de los plazos establecidos, las recomendaciones emitidas por la Auditoría Interna para implementarlas dentro de las operaciones que se llevan a cabo, o bien proponer medidas alternativas que reduzcan o eliminen las situaciones de riesgo determinadas y no se mantenga la exposición al riesgo sobre las operaciones que se llevan a cabo en forma diaria en la Institución, con las posibles implicaciones que ellas pueden originar sobre el patrimonio y los recursos públicos que administra la Junta de Protección Social, y el efecto que dichas situaciones pueden tener sobre los acreedores de rentas, que de materializarse expone a los titulares y subordinados a las sanciones que dispone el artículo N° 39 de la Ley General de Control Interno N° 8292.

# 1. INTRODUCCION.

## 1.1. Antecedentes del estudio.

El presente estudio fue desarrollado en cumplimiento al Plan Anual de Trabajo para el año 2018.

## 1.2. Objetivo general del estudio.

Verificar los planes de continuidad elaborados por el Departamento de Tecnologías de Información sobre los sistemas informáticos utilizados en los procesos institucionales.

## 1.3. Objetivos específicos

- Determinar el cumplimiento de los procedimientos y políticas establecidas para los planes de contingencia en la Junta de Protección Social.
- Analizar las pruebas realizadas en la Institución a los planes de continuidad.
- Verificar la valoración de riesgos relacionados a las acciones definidas en los planes de contingencia.

## 1.4. Alcance del estudio.

El estudio abarco la revisión de la documentación generada por el Departamento de Tecnologías de la Información en los años 2017 y 2018, en lo respecta a planes de continuidad.

## 1.5. Metodología.

Para la realización de este estudio se consultó:

a) Ley General de Control Interno N° 8292 del 18 de julio del 2002, en cuanto a los artículos N° 8, N° 10, Nº 15 y N° 16, referidos al Sistema de Control Interno.

b) Normas de Control Interno para el Sector Público, (Publicado en La Gaceta N° 26 del 6 de febrero del 2009), Normas Nº 1.4, Nº 1.5 N° 4.3, N° 4.4, N° 5.4, Nº 5.5 y Nº 5.6 sobre Responsabilidad de los Jerarcas y Titulares Subordinados respecto al Sistema de Control Interno, Protección y conservación del patrimonio, Exigencia de confiabilidad y oportunidad de la información, Gestión documental, Archivo Institucional y Calidad de la información.

c) Normas Técnicas para la gestión y Control de las tecnologías de información.

d) Manual de procedimientos de TI-JPS.

e) Manual Políticas de Administración TI-JPS, POLÍTICA DE CONTINUIDAD DE TI.

f) Estudio 04-2016 *"Verificación de la seguridad e integridad de las aplicaciones informáticas, bases de datos, conectividad y otros aspectos relacionados con la comercialización de la lotería electrónica adjudicada al consorcio GTECH-BOLDT GAMING"* y 23-2017 *"Consultoría técnica especializada para verificar la seguridad y planes de contingencia implementados por el departamento de tecnologías de la información en los servidores, dispositivos de red, base de datos y aplicaciones informáticas".*

g) ISO 22301 y ISO 27301, referentes a mejores prácticas para la continuidad de los servicios de TI.

h) JPS-GG-TI-0889-2018.

Para llevar a cabo el presente estudio se siguieron los sucesivos procedimientos:

- Recolección de correspondencia y otra documentación relacionada con la comunicación de los estándares y políticas.
- Recopilación de la normativa relacionada con el tema en estudio.
- Revisión de las políticas, procedimientos y estándares.
- Revisión de la Valoración de Riesgo efectuada por la Administración Activa sobre el área o proceso sujeto a estudio.
- Seguimiento de las recomendaciones pendientes sobre continuidad, establecidos en los informes 04-2016 y 23-2017.

Las actividades fueron realizadas de acuerdo con las normativas aplicables al ejercicio de la auditoría interna.

### 1.6. Normativa sobre deberes en el trámite de informes de Auditoría.

De conformidad con lo que establece la Contraloría General de la República, se transcriben los artículos Nº 36, Nº 37, Nº 38 y Nº 39 de la Ley General de Control Interno Nº 8292, publicada en la Gaceta Nº 169 de 4 de setiembre del 2002:

***"Artículo 36.- Informes dirigidos a los titulares subordinados***

*Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera:*

*a) El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados.*

*b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además, deberá ordenar la implantación de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes.*

*c) El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda.*

***Artículo 37.- Informes dirigidos al jerarca***

*Cuando el informe de auditoría esté dirigido al jerarca, este deberá ordenar al titular subordinado que corresponda, en un plazo improrrogable de treinta días hábiles contados a partir de la fecha de recibido el informe, la implantación de las recomendaciones. Si discrepa de tales recomendaciones, dentro del plazo indicado deberá ordenar las soluciones alternas que motivadamente disponga; todo ello tendrá que comunicarlo debidamente a la auditoría interna y al titular subordinado correspondiente.*

***Artículo 38.- Planteamiento de conflictos ante la Contraloría General de la República***

*Firme la resolución del jerarca que ordene soluciones distintas de las recomendadas por la auditoría interna, esta tendrá un plazo de quince*

*días hábiles, contados a partir de su comunicación, para exponerle por escrito los motivos de su inconformidad con lo resuelto y para indicarle que el asunto en conflicto debe remitirse a la Contraloría General de la República, dentro de los ocho días hábiles siguientes, salvo que el jerarca se allane a las razones de inconformidad indicadas.*

*La Contraloría General de la República dirimirá el conflicto en última instancia, a solicitud del jerarca, de la auditoría interna o de ambos, en un plazo de treinta días hábiles, una vez completado el expediente que se formará al efecto. El hecho de no ejecutar injustificadamente lo resuelto en firme por el órgano contralor, dará lugar a la aplicación de las sanciones previstas en el capítulo V de la Ley Orgánica de la Contraloría General de la República, N° 7428, de 7 de setiembre de 1994.*

***Artículo 39.- Causales de responsabilidad administrativa***

*El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios..."*

## 2. RESULTADOS DEL ESTUDIO.

### 2.1. Seguimiento de recomendaciones sobre planes de continuidad emitidos en informes anteriores.

En los informes 04-2016 *"Verificación de la seguridad e integridad de las aplicaciones informáticas, bases de datos, conectividad y otros aspectos relacionados con la comercialización de la lotería electrónica adjudicada al consorcio GTECH-BOLDT GAMING"* y 23-2017 *"Consultoría técnica especializada para verificar la seguridad y planes de contingencia implementados por el departamento de tecnologías de la información en los servidores, dispositivos de red, base de datos y aplicaciones informáticas"*, se extraen las recomendaciones relacionadas con los procesos de continuidad de negocio, los cuales se resumen de la siguiente manera:

**Tabla 1.** Recomendaciones del informe 04-2016 relacionadas con procesos de continuidad del negocio y su estado:

| AI JPS N° 04-2016 | Estado |
|---|---|
| a. Elaboren planes de recuperación de desastres donde se detallen las actividades que debe realizar el personal técnico para la recuperación de los sistemas críticos, de manera que los mismos ayuden a recuperar los servicios en los tiempos definidos sin causar daños importantes a la empresa. | Pendiente |

Fi: Informe N°04-2016.

**Tabla 2**. Recomendaciones del informe 23-2017 relacionadas con procesos de continuidad del negocio y su estado:

| AI JPS N° 23-2017 | Estado |
|---|---|
| c. Administrar los riesgos tecnológicos y monitorizarlos constantemente. Adicionalmente, se recomienda que se documente una metodología para la gestión de riesgos que incluya el análisis de riesgos, la evaluación de los riesgos, el plan de tratamiento de riesgos y seguimiento a las acciones acordadas y aprobadas. Cabe resaltar, que una gestión de riesgos adecuada es el punto de partida para poder salvaguardar los activos más valiosos de la institución. | Pendiente |
| 2. Fortalecer la Gestión de la Continuidad del Negocio, a través de las siguientes actividades: | Pendiente |
| a. Definir roles y responsabilidades para todo el ciclo de gestión de continuidad del negocio lo cual permitirá dar mantenimiento a todos los procedimientos, planes, políticas, manuales, protocolos y pruebas que permitan asegurar la continuidad de los servicios y procesos críticos. | Pendiente |
| b. Valorar la situación de los contratos vencidos con los proveedores críticos bien sea para renovarlos o reducir la dependencia con terceros. Una alternativa para reducir la dependencia puede ser capacitar al personal de la institución e incluir cláusulas en los contratos relacionadas a la prestación del servicio a la JPS durante una contingencia por parte del proveedor. | Pendiente |
| c. Se recomienda que el Departamento de Tecnologías de la Información desarrolle estrategias de continuidad y recuperación ante desastres, justificadas en: | Pendiente |

| | |
|---|---|
| El análisis de impacto en el negocio que permita identificar los servicios y/o procesos críticos de la institución, así como los objetivos de recuperación más adecuados para garantizar su supervivencia. | Pendiente |
| El análisis, evaluación y priorización de los riesgos que afectan la continuidad operativa y tecnológica de la Junta de Protección Social. | Pendiente |
| Las estrategias de continuidad que incluyan varias alternativas de recuperación para los servicios categorizados como críticos en el Análisis de Impacto al Negocio y con base en los riesgos detectados en el análisis de riesgos. Se recomienda que estas estrategias estén sustentadas con un caso de negocio que incluya el análisis costo beneficio y la justificación para invertir en la estrategia propuesta. | Pendiente |
| Dentro de las estrategias de continuidad se podrían establecer, por ejemplo: procedimientos manuales de recuperación, contratos con proveedores, respaldos diarios o en tiempo real, implementación de redundancia geográfica (podría ser a través de centros de datos alternos hot site, warm site o cold site), entre otros. | Pendiente |
| d. Se recomienda diseñar los planes de continuidad una vez las estrategias se encuentren aprobadas e implementadas, ya que, en caso contrario, se realizaría en plan bajo escenarios poco realistas que no aseguran la continuidad de las operaciones en caso de un evento no planificado. | Pendiente |

Fi: Informe N°23-2017.

Es importante destacar que las recomendaciones van enfocadas a fortalecer el proceso de continuidad del negocio desde el análisis de los diferentes riesgos, la participación de la administración activa en los procesos de definición de las áreas críticas, así como de los diferentes enfoques en la ejecución de dichos planes.

## 2.2. Pruebas de los planes de continuidad

En la política de continuidad de TI, se establece el proceso de realización de las pruebas de la siguiente manera: "*El Encargado de Continuidad deberá ejecutar pruebas de la infraestructura tecnológica crítica al menos una vez al año.*"

La ejecución de los procesos de pruebas o simulaciones controladas de los planes de continuidad, son necesarios para tener bien definido las responsabilidades de cada uno de los funcionarios y permite detectar fallas en el

diseño y así proponer planes de mejora para los mismos. Así mismo se puede evaluar el equipo y personal a cargo de cada actividad crítica.

En nota JPS-GG-TI-0889-2018 del 19 de noviembre del presente, el señor Ronald Ortiz Méndez, Jefe del Departamento de Tecnologías de la Información, establece la última prueba de los planes de contingencia en el periodo 2014, como se indicó en dicha nota:

> *"…las últimas pruebas realizas de la ejecución del Plan de Continuidad, se elaboraron en el periodo 2014, no se ha logrado realizar nuevamente, por cuanto se encuentra en trámite las contrataciones para el mantenimiento preventivo, correctivo y monitoreo de la infraestructura tecnológica…".*

La justificación que indica el señor Ortiz Méndez, se debe a que no se ha podido realizar las pruebas de los planes de continuidad en los periodos 2015-2016 y 2017, esto debido a que no se cuenta con los contratos vigentes de los diferentes proveedores, sin embargo, en consulta realizada al sistema de compras institucionales y al Departamento de Recursos Materiales, los contratos que indico el señor Ortiz Méndez se encuentran vigentes a dichos años, como se muestra a continuación:

1. *Licitación Abreviada No. 2014LA-000006-PROV por Mantenimiento al Motor de Base de Datos Sybase sobre SO Solaris y SO Windows Server adjudicado a Corporación Informática ODS S.A. Vigencia del contrato un año con posibilidad de prórroga por un año adicional. Fecha de inicio febrero 2015, fecha de finalización 31 de enero 2017.*

2. *Licitación Abreviada No. 2014LA-000006-PROV por Mantenimiento motor replicador RS adjudicado a SOIN Soluciones Integrales S.A. Vigencia del contrato un año con posibilidad de prórroga por un año adicional. Fecha de inicio 09 de marzo 2015, fecha de finalización 08 de marzo 2017.*

3. *Licitación Abreviada No. 2013LA-000019-PROV por Mantenimiento de unidades UPS adjudicado a Soporte Critico S.A. Vigencia del contrato un año con posibilidad de prórroga por tres años adicionales. Fecha de inicio 06 de junio 2014, fecha de finalización 05 de junio 2017.*

4. *Licitación Abreviada No. 2013LA-000021-PROV por Mantenimiento del equipo SUN Solaris adjudicado a Control Electrónico S.A. Vigencia del contrato un año con posibilidad de prórroga por tres años adicionales. Fecha de inicio 04 de octubre 2013, fecha de finalización 03 de abril 2017.*

5. *Licitación Abreviada No. 2015LA-000009-PROV sobre el contrato de servicios de mantenimiento preventivo y correctivo centro de datos principal adjudicado a Control Electrónico S.A. Vigencia del contrato un año con*

*posibilidad de prórroga por tres años adicionales. Fecha de inicio 01 de julio 2016, vigente a la fecha.*

En el informe N° 23-2017, se establece la siguiente recomendación:

"*b. Valorar la situación de los contratos vencidos con los proveedores críticos bien sea para renovarlos o reducir la dependencia con terceros. Una alternativa para reducir la dependencia puede ser capacitar al personal de la institución e incluir cláusulas en los contratos relacionadas a la prestación del servicio a la JPS durante una contingencia por parte del proveedor*"

Y las "Normas Técnicas para la gestión y Control de las tecnologías de información", en su "Capítulo III Implementación de tecnologías de información", "3.1 Consideraciones generales de la implementación de TI":

*"i. Promover su independencia de proveedores de hardware, software, instalaciones y servicios."*

En el punto "3.4 Contratación de terceros para la implementación y mantenimiento de software e infraestructura":

*"f. Implementar un proceso de transferencia tecnológica que minimice la dependencia de la organización respecto de terceros contratados para la implementación y mantenimiento de software e infraestructura tecnológica"*

La dependencia de terceros es un riesgo que debe ser controlado por el Departamento de Tecnologías de la Información, y, además, debe tener el personal interno capacitado y con el conocimiento necesario en el uso de las herramientas que manejan los proveedores para poder, en caso de ser necesario, activar los mecanismos de contingencia. Por lo tanto, la ejecución de los planes de continuidad debe de poderse implementar sin una dependencia directa de un proveedor.

## 2.3. Cumplimiento de las políticas de continuidad de Tecnologías de la Información

El plan de continuidad es un instrumento de gestión para el buen gobierno de las tecnologías de la información y las comunicaciones en el dominio del soporte y desempeño, estos planes contienen las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de una empresa, dada la importancia actual de las tecnologías modernas, el plan de contingencia es el más relevante de la Institución.

En la política de continuidad de las Tecnologías de la Información, se definieron las pruebas de continuidad de acuerdo al siguiente criterio:

> "*El Encargado de Continuidad deberá ejecutar pruebas de la infraestructura tecnológica crítica al menos una vez al año.*"

Por lo que, en las acciones descritas en el punto 2.2 de este informe, quedó en evidencia que la Institución lleva más de 3 (tres) años sin realizarlas.

Como se definió en las políticas de continuidad, por parte del Departamento de Tecnologías de la Información, se contempla una serie de insumos, tales como:

1. Análisis de riesgo (*El encargado de la continuidad de TI identificará y elaborará al menos una vez al año un informe el cual identifique los riesgos relacionados al proceso de continuidad de TI*)
2. Análisis de impacto del negocio (*El Encargado de Continuidad elaborará y actualizará el documento de análisis de impacto del negocio al menos una vez al año o cuando se presenten cambios significativos en la infraestructura tecnológica*)
3. La Estrategias de continuidad de tecnología (*El Encargado de Continuidad de TI con el apoyo del equipo de recuperación de tecnología evaluará al menos una vez al año las estrategias de continuidad*).
4. Capacitaciones (*El Encargado de Continuidad deberá capacitar al menos una vez al año al personal partícipe del proceso de continuidad de TI y sensibilizar al personal del área de TI sobre el proceso de continuidad*)

Los cuales son pilares fundamentales para mantener actualizados los planes de continuidad de negocio, mismos que fueron solicitados mediante oficio JPS-AI-942-2018 del 3 de diciembre del 2018 con el fin de examinarlos en la etapa de examen de la elaboración de este informe, sin embargo, a la fecha de conclusión del informe no hubo respuestas del Departamento de Tecnologías de la Información. Quedando este punto pendiente de revisión para un próximo estudio.

## 3. CONCLUSIONES.

La Auditoría Interna con fundamento en lo establecido en el artículo N° 22, inciso a) de la Ley General de Control Interno N° 8292, y en cumplimiento de su Programa Anual de Trabajo del Área de Sistemas de la Auditoría Interna para el período 2018, definió el estudio para verificar los planes de continuidad elaborados por el Departamento de Tecnologías de Información, esto con el objetivo de verificar los dichos planes de continuidad sobre los sistemas informáticos utilizados en los procesos institucionales.

Del presente estudio se determinó que existen recomendaciones pendientes de cumplir, las cuales fueron realizadas para el mejoramiento de los planes de

continuidad mediante la elaboración de los informes N°04-2016 *"Verificación de la seguridad e integridad de las aplicaciones informáticas, bases de datos, conectividad y otros aspectos relacionados con la comercialización de la lotería electrónica adjudicada al consorcio gtech-boldt gaming"* y N° 23-2017 "*Consultoría técnica especializada para verificar la seguridad y planes de contingencia implementados por el departamento de tecnologías de la información en los servidores, dispositivos de red, base de datos y aplicaciones informáticas*".

Además, se determinó que la Institución no ha realizado pruebas a dichos planes de continuidad desde hace tres años, la justificante que indicó el Departamento de Tecnologías de la Información se debe a que se depende completamente de los proveedores de servicio contratados por la Junta de Protección Social.

## 4. RECOMENDACIONES.

**Al señor Ronald Ortiz Méndez, Jefe del Departamento de Tecnologías de la Información:**

**4.1** Para las recomendaciones pendientes de cumplir de los informes N°04-2016 y N°23-2017, priorizar aquellas que se puedan ir atendiendo con el personal interno, de acuerdo al riesgo de cada una de ellas e informar de los avances a la Gerencia General.

**4.2** Cumplir con lo definido en la Política de Continuidad de Tecnologías de la Información, en lo que respecta a la realización de pruebas anuales a los planes de continuidad, sin tener dependencia directa de terceros.

ANDRES JOSE MARTINEZ PORRAS (FIRMA)
Firmado digitalmente por ANDRES JOSE MARTINEZ PORRAS (FIRMA)
Junta de Protección Social Auditoría Interna

**Realizado por:**
Andrés Martínez Porras
**Profesional II**

WEN JIE ZHEN WU (FIRMA)
Firmado digitalmente por WEN JIE ZHEN WU (FIRMA)
Junta de Protección Social Auditoría Interna

**Realizado por:**
Wen Jie Zhen Wu
**Profesional II**

JOSE ALBERTO WONG CARRION (FIRMA)
Firmado digitalmente por JOSE ALBERTO WONG CARRION (FIRMA)
Junta de Protección Social Auditoría Interna

**Revisado por:**
José Wong Carrión
**Jefe de Área**

RODRIGO CARVAJAL MORA (FIRMA)
Firmado digitalmente por RODRIGO CARVAJAL MORA (FIRMA)
Junta de Protección Social Auditoría Interna

**Aprobado por:**
Rodrigo Carvajal Mora
**Subauditor Interno**

miércoles 26/12/2018 14:27

José A. Wong Carrión <jwong@jps.go.cr>

**Adjunto nota de remisión N°1019 e informe N°19-2018 digital**

Para 'Ronald Ortiz Mendez'

CC 'Rodrigo Carvajal Mora'; 'Hazel Valverde Gonzalez'

19-2018 firmado.pdf
868 KB

1019-2018.pdf
440 KB

Buenas tardes

Adjunto encontrará nota N°1019 donde se remite el informe de auditoría N°19-2018 denominado *"Verificación y evaluación de los planes de continuidad de los servicios informáticos a nivel de la Junta de Protección Social"* el cual fue comunicado el día 21 de diciembre del presente.

Favor dar acuse de recibido

Gracias