TOME, 14 MAY 2024

VISTOS : Resolución Exenta N° 6 de 26.03.2019 de la Contraloría General de la República sobre exención de la Toma de Razón, Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma; en el Decreto Supremo Nº 83, del Ministerio Secretaría General de la Presidencia, de 2004, que aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos; en el Decreto Nº 14 de 2014 que modifica Decreto Nº 181, de 2002, que aprueba reglamento de la ley 19.799, y deroga los decretos que indica; en la ley 19.223 sobre delitos informáticos; en el Decreto Nº 83 de 28 de agosto de 2017, del Ministerio de Relaciones Exteriores que promulga Convenio sobre la Ciberdelincuencia; en la norma chilena NCh-ISO 27001. Of2013, Tecnología de la información – Técnicas de seguridad – Sistemas de Gestión de la seguridad de la información – requisitos; en el Instructivo Presidencial Nª8 que imparte instrucciones urgentes en materia de ciberseguridad, y Resolución Exenta N°2778 de fecha 24.08.2023, que Encomienda funciones de Director (s) Hospital de Tomé, y;

CONSIDERANDO: **PRIMERO** que, conforme dispone el Artículo 12 del Decreto Nº 83 de 2005 del Ministerio Secretaría General de la Presidencia "En cada organismo regido por esta norma deberá existir un encargado de seguridad, que actuará como asesor del Jefe de Servicio correspondiente en las materias relativas a seguridad de los documentos electrónicos.
Las funciones específicas que desempeñe internamente el encargado de seguridad serán establecidas en la resolución que lo designe. En todo caso, deberá tener, a lo menos, las siguientes funciones:
a) Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de su organización y el control de su implementación, y velar por su correcta aplicación.
b) Coordinar la respuesta a incidentes computacionales.
c) Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes".

SEGUNDO: Que, conforme al Instructivo Presidencial Nº 8 "que imparte instrucciones urgentes en materia de Ciberseguridad" de 23 de octubre de 2018, se requiere el nombramiento de una contraparte ministerial frente al Ministerio del Interior para estas materias.

TERCERO: Que según lo establecido en el Decreto N°273 del Ministerio del Interior y Seguridad Pública, del 13 de septiembre del 2022, se establece la siguiente función "Los jefes de servicio de los Ministerios y demás organismos de la Administración centralizada y descentralizada del Estado deberán comunicar los incidentes de ciberseguridad que les afecten, al Ministerio del Interior y Seguridad Pública, mediante su notificación al Centro de Respuesta ante Incidentes de Seguridad Informática ("CSIRT"), en el sitio web https://csirt.gob.cl."

CUARTO: Que, en consecuencia, existe la necesidad de perfeccionar la estructura Funcional de la Ciberseguridad y seguridad de la información para el HOSPITAL DE TOMÉ, por lo que, dicto la siguiente:

RESOLUCION EXENTA Nº 847

1.- ENCOMIENDASE a contar de 01 de Mayo del 2024 a D. **CÉSAR ANTONIO CÁCERES URRUTIA**, Cedula de Identidad Nº 15.854.658-2, Profesional grado 11° EUS, Calidad Jurídica Contrata, el cargo de ***"ENCARGADO DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN DEL HOSPITAL DE TOMÉ".***

2.- ASÍGNASE, las siguientes funciones al Encargado de Ciberseguridad y Seguridad de la Información:

a) Liderar las iniciativas en materias de seguridad de la información, plantearlas al comité de seguridad de la información, y mantener informado al jefe de servicio, de los acuerdos establecidos en estos escenarios.

b) Velar por la ciberseguridad, y actuar frente a infracciones a la privacidad y amenazas, sus tendencias y escenarios estratégicos que pudieren afectar al Ministerio de Salud.

c) Alinear los esfuerzos de las distintas áreas de la Institución, respecto a la protección de los sistemas tecnológicos y a la información contenida en ellos, según los criterios de Ciberseguridad.

d) Gestionar internamente el tratamiento de los incidentes que estén vinculados a los activos de información de la institución, identificados y/o reportados tanto por el Ministerio del Interior como por
instancias internas del Ministerio y la Red de Salud, efectuando la Re portabilidad y el seguimiento adecuado de dichos eventos.

e) Apoyar el proceso de sensibilización en materias de ciberseguridad al interior de la institución. Organizando actividades de concientización y capacitación en seguridad para educar a los funcionarios sobre buenas prácticas y comportamientos seguros.

f) Organizar y presidir el comité de seguridad de la información, que tendrá a su cargo la actualización de políticas y procedimientos, de Ciberseguridad y Seguridad de la Información de la institución, el control de su implementación, y velar por su correcta aplicación.

g) Coordinar las acciones necesarias para resguardar y asegurar la continuidad del negocio frente a incidentes de Ciberseguridad.

h) Resguardar que se informe adecuadamente a todas las personas naturales y jurídicas que puedan tener acceso a los activos de información de la institución, acerca de las Políticas de Ciberseguridad y Seguridad de la Información vigentes, y en particular sobre las obligaciones que le correspondan en relación a la gestión de incidentes.

i) Comunicar los incidentes de ciberseguridad de los que tenga conocimiento en ejercicio de sus funciones, al Ministerio del Interior y Seguridad Pública, mediante su notificación al Centro de Respuesta ante Incidentes de Seguridad Informática ("CSIRT"), en el sitio web: https://csirt.gob.cl, en representación del jefe del servicio, en su calidad de autoridad máxima de la institución.

j) Establecer puntos de enlace con encargados de seguridad de la información y ciberseguridad, de otros organismos públicos y especialistas externos, que le permitan estar al tanto de las tendencias, normas y métodos en estas materias.

k) Definir políticas y procedimientos de seguridad de la información y ciberseguridad, así como un plan de acción para mitigar riesgos y proteger los sistemas y datos de la organización.

l) Apoyar en la identificación, evaluación y gestión de los riesgos de seguridad de la información del Ministerio de Salud, realizando evaluaciones periódicas de vulnerabilidades y amenazas. Implementando controles y medidas para minimizar la exposición a riesgos potenciales y proteger los activos críticos.

m) Encargado de implementar y mantener los controles de seguridad adecuados para proteger la infraestructura, los sistemas y los datos. Esto puede incluir firewalls, sistemas de detección de intrusos, sistemas de prevención de pérdida de datos y otros mecanismos de seguridad.

n) Evaluar la seguridad de proveedores y terceros con acceso a información sensible de la organización para asegurarse de que cumplan con los estándares de seguridad requeridos.

3.- DEJASE ESTABLECIDO que a contar del 01 de mayo de 2024 a D. **LEANDRO ERNESTO CUADRA VERA**, Cedula de Identidad Nº 15.519.997-0, Profesional grado 15° EUS, Calidad Jurídica Contrata, como ***"ENCARGADO SUBROGANTE DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN DEL HOSPITAL DE TOME".***

4.- Se deja establecido que la designación no libera a los profesionales funcionarios antes citados del cumplimiento de sus funciones habituales y es sin derecho a mayor remuneración.

5.- PUBLÍQUESE, La presente Resolución para su adecuado conocimiento y difusión a todos los funcionarios, en la página web del Hospital de Tomé.

"ANÓTESE Y COMUNÍQUESE"

SERVICIO DE SALUD TALCAHUANO * HOSPITAL TOMÉ * DIRECTOR

ANIBAL CEA HENRIQUEZ
DIRECTOR (S)
HOSPITAL DE TOME

P.P.

ACH/BEM/CMB/RBB/msg
N° Int.443/10/05/2024
DISTRIBUCION:

- Dirección
- Subdirección Administrativa Hosp. Tomé
- Subdirección Medica Hosp.Tome
- Unidad de Personal Hosp. Tomé
- Interesados
- Jefes Áreas y C.R Hosp.Tomé
- Oficina de Partes

TOME, 14 MAY 2024

VISTOS : Resolución Exenta N° 6 de 26.03.2019 de la Contraloría General de la República sobre exención de la Toma de Razón, Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma; en el Decreto Supremo Nº 83, del Ministerio Secretaría General de la Presidencia, de 2004, que aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos; en el Decreto Nº 14 de 2014 que modifica Decreto Nº 181, de 2002, que aprueba reglamento de la ley 19.799, y deroga los decretos que indica; en la ley 19.223 sobre delitos informáticos; en el Decreto Nº 83 de 28 de agosto de 2017, del Ministerio de Relaciones Exteriores que promulga Convenio sobre la Ciberdelincuencia; en la norma chilena NCh-ISO 27001. Of2013, Tecnología de la información – Técnicas de seguridad – Sistemas de Gestión de la seguridad de la información – requisitos; en el Instructivo Presidencial Nª8 que imparte instrucciones urgentes en materia de ciberseguridad, y Resolución Exenta N°2778 de fecha 24.08.2023, que Encomienda funciones de Director (s) Hospital de Tomé, y;

CONSIDERANDO: **PRIMERO** que, conforme dispone el Artículo 12 del Decreto Nº 83 de 2005 del Ministerio Secretaría General de la Presidencia "En cada organismo regido por esta norma deberá existir un encargado de seguridad, que actuará como asesor del Jefe de Servicio correspondiente en las materias relativas a seguridad de los documentos electrónicos.
Las funciones específicas que desempeñe internamente el encargado de seguridad serán establecidas en la resolución que lo designe. En todo caso, deberá tener, a lo menos, las siguientes funciones:
a) Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de su organización y el control de su implementación, y velar por su correcta aplicación.
b) Coordinar la respuesta a incidentes computacionales.
c) Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes".

SEGUNDO: Que, conforme al Instructivo Presidencial Nº 8 "que imparte instrucciones urgentes en materia de Ciberseguridad" de 23 de octubre de 2018, se requiere el nombramiento de una contraparte ministerial frente al Ministerio del Interior para estas materias.

TERCERO: Que según lo establecido en el Decreto N°273 del Ministerio del Interior y Seguridad Pública, del 13 de septiembre del 2022, se establece la siguiente función "Los jefes de servicio de los Ministerios y demás organismos de la Administración centralizada y descentralizada del Estado deberán comunicar los incidentes de ciberseguridad que les afecten, al Ministerio del Interior y Seguridad Pública, mediante su notificación al Centro de Respuesta ante Incidentes de Seguridad Informática ("CSIRT"), en el sitio web https://csirt.gob.cl."

CUARTO: Que, en consecuencia, existe la necesidad de perfeccionar la estructura Funcional de la Ciberseguridad y seguridad de la información para el HOSPITAL DE TOMÉ, por lo que, dicto la siguiente:

RESOLUCION EXENTA Nº 847

1.- ENCOMIENDASE a contar de 01 de Mayo del 2024 a D. **CÉSAR ANTONIO CÁCERES URRUTIA**, Cedula de Identidad Nº 15.854.658-2, Profesional grado 11° EUS, Calidad Jurídica Contrata, el cargo de "***ENCARGADO DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN DEL HOSPITAL DE TOMÉ".***

2.- ASÍGNASE, las siguientes funciones al Encargado de Ciberseguridad y Seguridad de la Información:

a) Liderar las iniciativas en materias de seguridad de la información, plantearlas al comité de seguridad de la información, y mantener informado al jefe de servicio, de los acuerdos establecidos en estos escenarios.

b) Velar por la ciberseguridad, y actuar frente a infracciones a la privacidad y amenazas, sus tendencias y escenarios estratégicos que pudieren afectar al Ministerio de Salud.

c) Alinear los esfuerzos de las distintas áreas de la Institución, respecto a la protección de los sistemas tecnológicos y a la información contenida en ellos, según los criterios de Ciberseguridad.

d) Gestionar internamente el tratamiento de los incidentes que estén vinculados a los activos de información de la institución, identificados y/o reportados tanto por el Ministerio del Interior como por
instancias internas del Ministerio y la Red de Salud, efectuando la Re portabilidad y el seguimiento adecuado de dichos eventos.

e) Apoyar el proceso de sensibilización en materias de ciberseguridad al interior de la institución. Organizando actividades de concientización y capacitación en seguridad para educar a los funcionarios sobre buenas prácticas y comportamientos seguros.

f) Organizar y presidir el comité de seguridad de la información, que tendrá a su cargo la actualización de políticas y procedimientos, de Ciberseguridad y Seguridad de la Información de la institución, el control de su implementación, y velar por su correcta aplicación.

g) Coordinar las acciones necesarias para resguardar y asegurar la continuidad del negocio frente a incidentes de Ciberseguridad.

h) Resguardar que se informe adecuadamente a todas las personas naturales y jurídicas que puedan tener acceso a los activos de información de la institución, acerca de las Políticas de Ciberseguridad y Seguridad de la Información vigentes, y en particular sobre las obligaciones que le correspondan en relación a la gestión de incidentes.

i) Comunicar los incidentes de ciberseguridad de los que tenga conocimiento en ejercicio de sus funciones, al Ministerio del Interior y Seguridad Pública, mediante su notificación al Centro de Respuesta ante Incidentes de Seguridad Informática ("CSIRT"), en el sitio web: https://csirt.gob.cl, en representación del jefe del servicio, en su calidad de autoridad máxima de la institución.

j) Establecer puntos de enlace con encargados de seguridad de la información y ciberseguridad, de otros organismos públicos y especialistas externos, que le permitan estar al tanto de las tendencias, normas y métodos en estas materias.

k) Definir políticas y procedimientos de seguridad de la información y ciberseguridad, así como un plan de acción para mitigar riesgos y proteger los sistemas y datos de la organización.

l) Apoyar en la identificación, evaluación y gestión de los riesgos de seguridad de la información del Ministerio de Salud, realizando evaluaciones periódicas de vulnerabilidades y amenazas. Implementando controles y medidas para minimizar la exposición a riesgos potenciales y proteger los activos críticos.

m) Encargado de implementar y mantener los controles de seguridad adecuados para proteger la infraestructura, los sistemas y los datos. Esto puede incluir firewalls, sistemas de detección de intrusos, sistemas de prevención de pérdida de datos y otros mecanismos de seguridad.

n) Evaluar la seguridad de proveedores y terceros con acceso a información sensible de la organización para asegurarse de que cumplan con los estándares de seguridad requeridos.

3.- DEJASE ESTABLECIDO que a contar del 01 de mayo de 2024 a D. **LEANDRO ERNESTO CUADRA VERA**, Cedula de Identidad Nº 15.519.997-0, Profesional grado 15° EUS, Calidad Jurídica Contrata, como ***"ENCARGADO SUBROGANTE DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN DEL HOSPITAL DE TOME".***

4.- Se deja establecido que la designación no libera a los profesionales funcionarios antes citados del cumplimiento de sus funciones habituales y es sin derecho a mayor remuneración.

5.- PUBLÍQUESE, La presente Resolución para su adecuado conocimiento y difusión a todos los funcionarios, en la página web del Hospital de Tomé.

"ANÓTESE Y COMUNÍQUESE"

SERVICIO DE SALUD TALCAHUANO * HOSPITAL TOME * DIRECTOR (S)

ANIBAL CEA HENRIQUEZ
DIRECTOR (S)
HOSPITAL DE TOME

TRANSCRITO FIELMENTE

ACH/BEM/CMB/RBB/msg
N° Int.443/10.05.2024
DISTRIBUCION:

- Dirección
- Subdirección Administrativa Hosp. Tomé
- Subdirección Medica Hosp.Tome
- Unidad de Personal Hosp. Tomé
- Interesados
- Jefes Áreas y C.R Hosp.Tomé
- Oficina de Partes

SERVICIO DE SALUD TALCAHUANO * HOSPITAL DE TOME * MINISTRO DE FE