Memorando
CEM-41-2020

1 de junio de 2020

A: Lissette Montoya Gamboa
Subgerencia

DE: Ema Rebeca Alfaro Araya
Contraloría Empresarial

ASUNTO: Advertencia, riesgos por trabajo en casa.

Se remite el informe CEM-2020-IF-013, en el que se presenta una advertencia emitida por esta CEM respecto a los riesgos que enfrenta la ESPH tras la implementación de la modalidad de trabajo en casa, como consecuencia de la emergencia nacional por el virus COVID-19.

Muchas gracias.

Copia: Ana Yanci Herrera Murillo
Vanessa Mejia Mejia
Luis Enrique Salas Esquivel
Ingrid Rodriguez
Daisy Villalobos Cruz
Maikol Fernando Hernández Segura
Miguel Barrantes Arguello
Gustavo Adolfo Narváez Reyes
Meredith Torres Castro

Anexos: CEM-2020-IF-013

Creado por Jenny Campos Arrieta

29 de mayo de 2020
CEM-2020-IF-013

CONTRALORÍA EMPRESARIAL

ADVERTENCIA ACERCA DE LOS RIESGOS DE LA MODALIDAD DE TRABAJO EN CASA, DADA LA EMERGENCIA POR LA ENFERMEDAD COVID-19

Remitido mediante el memorando CEM-41-2020

Contraloría Empresarial Firmas de validación		
Realizado por		**Seguimiento de recomendaciones**
Debido a la emergencia nacional por la enfermedad COVID-19, no es posible registrar sus firmas.		
Maikol Hernández Segura Auditor de TI	*Miguel Barrantes Argüello Auditor de TI*	*Gustavo Narváez Reyes Auditor Interno encargado*
Revisado por		**Aprobado por**
Debido a la emergencia nacional por la enfermedad COVID-19, no es posible registrar su firma.		X
Daisy Villalobos Cruz Directora de Auditoría		*Ema Rebeca Alfaro Araya Contralora Empresarial*

TABLA DE CONTENIDOS

TABLA DE ABREVIATURAS

Abreviatura	Significado
AA	Administración Activa
CATIC	Comité de Arquitectura Tecnológica
CEM	Contraloría Empresarial
CGR	Contraloría General de la República
DOSTE	Macroproceso de Desarrollo, Operación y Soporte Tecnológico
ESPH	Empresa de Servicios Públicos de Heredia S.A.
GG	Gerencia General de la ESPH
JD	Junta Directiva de la ESPH
LGCI	Ley General de Control Interno n.° 8292
VPN	Virtual Private Network
RIO	Red de Información Oficial de la ESPH
SYSO	Salud y Seguridad Ocupacional

1. ASPECTOS INTRODUCTORIOS

Se detallan los antecedentes, el objetivo, la fundamentación, la aclaración de otras competencias, el cumplimiento de la normativa y el análisis de riesgos de este informe[1].

1.1. Antecedentes

Deben considerarse los siguientes aspectos:

- Se emite el Decreto n.° 39225 publicado en la Gaceta n.° 204 del 21 de octubre de 2015, que busca posicionar el teletrabajo como un medio impulsor de las acciones de modernización en las instituciones del sector público.
- El 18 de setiembre de 2019, se publica la Ley para regular el teletrabajo n.° 9738 que pretende promover, regular e implementar el teletrabajo como instrumento para generar empleo y modernizar las organizaciones públicas y privadas, a través del uso de tecnologías de la información y comunicación.
- Como medida para enfrentar la crisis mundial generada por el virus COVID-19, el 9 de marzo de 2020 la Presidencia de la República gira directrices a las instituciones públicas para enviar a teletrabajo a las personas cuyas funciones se pueden realizar de manera remota y se insta a la empresa privada a hacer lo mismo.
- Con instrucciones de la Subgerencia mediante correo electrónico se define que se habilitará la opción de trabajo remoto mediante VPN a las personas funcionarias que pertenecen a la lista de alto riesgo suministrada por Gestión y Desarrollo Humano de forma prioritaria.
- El 15 de abril de 2020, en sesión del Comité Gerencial Informático se presenta el Informe de Resultados referente a la habilitación del trabajo remoto para los funcionarios de la ESPH, elaborado por el DOSTE.
- En las primeras horas de la mañana del 14 de mayo de 2020, se presentan dificultades para acceder a los sistemas de la ESPH en general, ya que no es posible el ingreso al primer nivel de registro en la red (dominio). Se sospecha de un ataque informático realizado por medio del servicio de VPN implementado.
- El 15 de mayo de 2020, se comunica la recuperación del último respaldo en un nuevo servidor, sin embargo, el servicio mostraba cierta inestabilidad, por lo que persisten problemas de acceso a los sistemas para trabajar con normalidad. Se procede con la creación de nuevas cuentas de VPN para quienes tienen computadoras portátiles de la ESPH y se deshabilita el acceso para las personas funcionarias que utilizan laptops personales.
- En la semana del 18 al 22 de mayo de 2020, se conoce que la recuperación del servicio de acceso se atrasó porque se reinstaló el servicio desde cero ante la posibilidad de la existencia de puertas traseras (backdoor) insertadas por los supuestos atacantes informáticos.

[1] No corresponde a un informe de Control Interno o de Auditoría, tal como se conceptualiza en la LGCI, Capítulo IV “La auditoría interna”, Sección IV “Informes de auditoría interna”, artículos n.° 35 al 38.

1.2. Objetivo

Advertir a Desarrollo y Soporte Tecnológico acerca de la necesidad de realizar el análisis y las acciones de administración de los riesgos actuales que posee la ESPH, debido la implementación de la modalidad de trabajo en casa por la emergencia sanitaria del virus COVID-19.

1.3. Fundamentación

De acuerdo con la LGCI, se establece[2]:

> Artículo 22. —**Competencias**. Compete a la auditoría interna, primordialmente lo siguiente:
>
> d) Asesorar, en materia de su competencia, al jerarca del cual depende; además, advertir a los órganos pasivos que fiscaliza sobre las posibles consecuencias de determinadas conductas o decisiones, cuando sean de su conocimiento.

El pronunciamiento de la CGR n.° 5202, del 20 de mayo de 2003, indica lo siguiente:

> **La asesoría**: consiste en proveer al jerarca criterios, opiniones u observaciones que coadyuven a la toma de decisiones. Puede brindarse en forma oral pero de preferencia debe ser escrita, y se emite a solicitud de la parte interesada, sobre asuntos estrictamente de su competencia…

1.4. Aclaración de otras competencias

Esta CEM se reserva la posibilidad de verificar, por los medios que considere pertinentes, la efectiva implementación de los recordatorios de la normativa, de las observaciones y de valorar la solicitud de establecer las responsabilidades que correspondan, en caso de su incumplimiento injustificado.

1.5. Cumplimiento de la normativa

De acuerdo con las Normas para el Ejercicio de la Auditoría Interna en el Sector Público, emitidas por la CGR (NEAISP, punto 1.1.3), así como los resultados de la Autoevaluación de la Calidad de la CEM de 2018 (realizada en 2019[3]), las labores de la CEM y de esta advertencia son "*realizadas de acuerdo con la normativa aplicable al ejercicio de la auditoría interna*".

1.6. Análisis de Riesgos

Se presenta el análisis de riesgos con respecto a la situación analizada:

Aspecto	Análisis de Riesgos		
	Probabilidad	Impacto	Riesgo
Trabajo en casa por parte de los funcionarios de la ESPH, debido a la emergencia por COVID-19	2	3	**6**

[2] Esta CEM utiliza cuadros de texto para enmarcar las citas textuales, tal como lo utilizan algunos libros de texto, dado que facilita la comprensión para la persona lectora.
[3] Informe CEM-2019-IF-004, remitido con el memorando CEM-65-2019.

Área por evaluar	Descripción del Riesgo	Nivel
Cultura organizacional de la ESPH	Si no se capacita de manera adecuada al personal de la ESPH (conexión a redes inseguras, mecanismos para prevenir el robo de información, ingeniería social, entre otros), los usuarios podrían no ser conscientes de los riesgos a los que pueden verse expuestos y de los cuidados que deben tener al ingresar dispositivos ajenos a la compañía. Se puede generar robo o pérdida de información por medio de engaños basados en ingeniería social.	Alto
Costo financiero del teletrabajo	Si no se realizan de forma oportuna las solicitudes en tarifas y presupuesto, que consideren la inversión necesaria para la adquirir la infraestructura para el desarrollo del teletrabajo, no será posible implementarla con eficacia ni eficiencia en la ESPH.	Alto
Gestión de la información	Si los dispositivos que almacenan información no se encuentran cifrados, terceros no autorizados podrían accederla.	Alto
	Se incrementa la posibilidad de robo o pérdida de información si no se regula el almacenamiento de información en las máquinas de los usuarios, ya que no se controla el uso de dispositivos de almacenamiento externo tipo USB y no se vigila el uso efectivo del Sistema de Control Documental ni de los ambientes híbridos de almacenamiento (nube).	Alto
Implementación de la infraestructura tecnológica para el teletrabajo	Si la ESPH no cuenta con los equipos de cómputo necesarios para implementar el teletrabajo, se debe permitir a las personas funcionarias utilizar sus propios equipos de cómputo y dispositivos portátiles, lo cual genera brechas de seguridad.	Alto
	Si los equipos de cómputo se conectan a los sistemas empresariales mediante redes inseguras, se pueden ejecutar “exploits” (programa o código que se aprovecha de un agujero de seguridad) y se genera una infección con código malicioso (virus, malware, spyware, keyloggers, troyanos, entre otros).	Alto
	Si existen aspectos técnicos que se encuentran bajo la responsabilidad del usuario de teletrabajo (configuración del router ubicado en el domicilio, escaneo de los dispositivos USB conectados a los equipos remotos, utilización del doble factor en los accesos a sistemas, entre otros), se forman brechas de seguridad que podrían ser explotadas por terceros.	Alto
	Si las herramientas actuales de monitoreo de la red no son las adecuadas para hacer un seguimiento del tipo de tráfico (desde donde se intenta realizar el acceso, si hay intentos recurrentes y fallidos de ingreso a servidores, generación de tráfico inapropiado como la descarga de archivos desconocidos, entre otros) fuera del perímetro físico de la ESPH, no será posible identificar los dispositivos de los usuarios que están ingresando a la red ni las acciones que ejecutan.	Alto

La valoración del riesgo mostrada en la tabla anterior es consistente con los objetivos establecidos en las Políticas Institucionales para la Administración del Riesgo, aprobadas mediante acuerdo de Junta Directiva JD 116-2008 del 29 de abril de 2008 y cuyo mapa de calor se observa de la siguiente forma:

MATRIZ DE RIESGOS

IMPACTO				
3	3	3	6	9
2	2	2	4	6
1	1	1	2	3
0	1	2	3	

PROBABILIDAD

6 - 9	Alta Probabilidad con Alto Impacto
3 - 5	Mediana Probabilidad con Mediano Impacto
1 - 2	Poca Probabilidad con Poco Impacto

2. DESARROLLO

Como un servicio preventivo de la Contraloría Empresarial, se efectúa la siguiente advertencia referente a los riesgos actuales relacionados con el trabajo en casa, producto de la emergencia por el COVID-19.

2.1. Conceptos claves

De conformidad con La Ley para regular el teletrabajo n.° 9738, se define *teletrabajo* como:

> ARTÍCULO 3- Definiciones
>
> a) Teletrabajo: modalidad de trabajo que se realiza fuera de las instalaciones de la persona empleadora, utilizando las tecnologías de la información y comunicación sin afectar el normal desempeño de otros puestos, de los procesos y de los servicios que se brindan. Esta modalidad de trabajo está sujeta a los principios de oportunidad y conveniencia, donde la persona empleadora y la persona teletrabajadora definen sus objetivos y la forma en cómo se evalúan los resultados del trabajo.

Dentro del mismo artículo, se definen dos tipos de teletrabajo según el lugar donde se desarrolle y los medios utilizados:

a) Teletrabajo domiciliario: Se da cuando las personas trabajadoras ejecutan sus actividades laborales desde su domicilio.

b) Teletrabajo móvil: Se produce cuando las personas trabajadoras realizan sus funciones de manera itinerante, ya sea en el campo o con traslados constantes, con ayuda del uso de equipos móviles que sean fácilmente utilizables y transportables.

El teletrabajo, además de ser autorizado por el responsable del proceso o superior jerárquico al cual pertenezca el usuario solicitante, también debe tener el visto bueno del proceso responsable de la seguridad de la información, que se encarga de velar por el cumplimiento de las políticas, normas y procedimientos existentes.

2.2. Situación encontrada

Desde el 9 de marzo de 2020, Costa Rica atraviesa una situación de emergencia como repercusión de la pandemia generada por el virus COVID-19. Por ello, el Ministerio de Salud ha dictado una serie de órdenes sanitarias a nivel país, entre ellas la disposición de que las empresas enviaran a todo el personal posible a trabajar en la casa para tener menor exposición al riesgo sanitario.

Mediante correo electrónico el 12 de marzo de 2020, y en acatamiento a la ordenanza del Ministerio de Salud, el área de Salud y Seguridad Ocupacional de la ESPH (SYSO) en conjunto con Subgerencia, han dispuesto la habilitación del trabajo remoto mediante VPN para las personas funcionarias de la lista de alto riesgo que Gestión y Desarrollo Humano suministra con prioridad.

De acuerdo con el concepto formal, lo que en este momento se realiza en la ESPH no es teletrabajo, sino que se han enviado a algunos miembros del personal a trabajar vía remota desde sus hogares. No obstante, a la luz del evento informático del 14 de mayo de 2020 (reseñado en los antecedentes), los riesgos presentes en el cuadro correspondiente se incrementaron.

Ahora bien, a pesar de la premura por la habilitación de los puestos de trabajo se considera necesario que la Administración efectúe algunas medidas complementarias para mitigar el riesgo o las vulnerabilidades que actualmente se tienen. Algunas de ellas son:

- Los requerimientos de seguridad de comunicaciones, que consideran la necesidad de acceso remoto a los sistemas internos de la ESPH y la sensibilidad de la información por acceder.
- La amenaza de acceso no autorizado a información o recursos por parte de otras personas que se encuentran presentes en el lugar donde se desarrolla el teletrabajo.
- Definición del trabajo permitido, el horario laboral y la clasificación de la información que se puede almacenar en el equipo remoto.
- Establecimiento de los sistemas internos y servicios a los cuales la persona funcionaria de la ESPH está autorizada a consultar.
- Definición de los procedimientos de respaldo de la información generada durante el teletrabajo.

- Anulación de las autorizaciones, derechos de acceso y devolución del equipo que pertenezca a la ESPH, una vez que finalicen formalmente las actividades remotas.
- Implementación de procesos de auditoría específicos para los casos de accesos remotos.

3. CONCLUSIÓN

La CEM advierte de la necesidad de un análisis profundo de los riesgos que tiene la ESPH de que parte de su personal trabaje desde sus casas, ya que no se ha implementado por completo la modalidad de teletrabajo.

Como consecuencia del análisis solicitado, es importante conocer las medidas que la Administración Activa ejecutará para mitigar los riesgos encontrados y establecer un ambiente adecuado, en términos de seguridad de la información.

En cuanto al evento del 14 de mayo de 2020, que impidió el acceso a los sistemas de la ESPH, se recomienda formular un informe de la situación presentada, que debe dirigirse hacia la Junta Directiva y la Gerencia General y que consigne aspectos como:

- Descripción detallada del evento, junto con sus causas y consecuencias.
- Análisis de la información recabada.
- Acciones ejecutadas para solventar la situación adversa.
- Limitaciones presentadas durante el evento.
- Herramientas utilizadas para su atención.
- En caso de que se trate de un ataque informático dirigido a la ESPH:
    - Identificar a los posibles vectores utilizados para su perpetración.
    - Establecer el proceso que debe realizarse en ese caso, con el fin de restaurar la operación y mitigar la exposición.
- Evidencia que respalde las conclusiones del informe (logs de sistemas informáticos, registros del sistema operativo, documentos electrónicos, comunicaciones electrónicas, entre otros).

Todo ello, serviría como insumo en caso de que la ESPH deba aplicar medidas de índole legal en respuesta al incidente.

4. ANEXO

4.1. Actuación respecto a esta advertencia

En cuanto a los servicios de Asesoría y Advertencia, la CGR ha establecido lo siguiente, mediante el oficio n.° 02836 del 23 de marzo de 2012:

> … debe indicarse que a pesar de que la advertencia no resulta de obligado acatamiento por parte del jerarca, es de esperar que éste actúe de manera congruente con la advertencia, toda vez que el artículo 12 de la LGCI le impone, entre otros, los siguientes deberes en su calidad de jerarca y responsable del adecuado funcionamiento del sistema de control interno:
>
> "b) Tomar de inmediato las acciones correctivas, ante cualquier evidencia de desviaciones o irregularidades.
>
> c) Analizar e implantar, de inmediato, las observaciones, recomendaciones y disposiciones formuladas por la auditoría interna, la CGR, la auditoría externa y las demás instituciones de control y fiscalización que correspondan."
>
> Esa regulación es congruente con el principio de eficiencia que recoge el artículo 10 de la Constitución Política, así como con otras regulaciones del ordenamiento que preceptúan la obligación del funcionario público de actuar de forma que su gestión permita una rendición de cuentas ajustada a derecho. Por ende, no sería aceptable que el funcionario conozca y archive la advertencia que le brinda la auditoría interna, sin haber analizado lo que se le comunica y haber manifestado razonadamente su decisión al respecto, toda vez que, siendo ya conocedor de las eventuales consecuencias de la acción o decisión, su inacción podría acarrearle las responsabilidades previstas en el artículo 39 de la LGCI, por debilitamiento del control interno o, en general, por incumplimiento de los deberes que le asigna la ley.
>
> Por consiguiente, debería esperarse que el destinatario de la advertencia adopte alguna acción válida a raíz de ella, o en caso de desechar lo comunicado por la auditoría interna, justifique claramente las razones atinentes. En ese sentido, si la advertencia se ha suministrado de manera verbal en el curso de una sesión o reunión, las manifestaciones de la administración al respecto deben quedar asentadas en el acta o en la minuta respectiva; si la comunicación de la advertencia ha tenido lugar mediante un documento formal, el órgano pasivo debería manifestar de igual modo lo pertinente a la auditoría interna; si no lo hace, tal omisión constituirá un elemento adicional a tomar en cuenta en el momento de efectuar el seguimiento respectivo, sin perjuicio de las reiteraciones que la auditoría interna estime conveniente cursar.
>
> Al respecto, conviene tener presente que la advertencia y las acciones subsecuentes no están sometidas al régimen previsto en los artículos 36 a 38 de la Ley General de Control Interno, pues éste se refiere únicamente a las recomendaciones planteadas en los estudios formales de auditoría. No obstante, sí es necesario que la auditoría interna verifique el proceder posterior de la administración, para determinar su legalidad y su propiedad técnica; ello puede realizarse como parte de un estudio de auditoría que incluya en su alcance, entre otros asuntos, los relativos a las acciones derivadas de las advertencias brindadas por la auditoría interna, o bien como un estudio especial que permita determinar la procedencia de lo actuado por la administración. Es claro que, dependiendo de cómo se realice este seguimiento, se obtendrán productos diferentes, ya sea un informe de control interno o uno de responsabilidad, según corresponda.

Debido a lo expuesto, esta CEM se permite solicitar la remisión de copias de los actos o disposiciones que se emitan al respecto.