Martes 12 de mayo, 2020
AI-0122-2020

Al contestar refiérase al número de oficio asignado a la presente comunicación; preferiblemente con el uso de firma digital, a través de la dirección correo electrónico auditoria.interna@sfe.go.cr

Ingeniero
Fernando Araya Alpízar, Director
Servicio Fitosanitario del Estado (SFE)

Licenciado
Didier Suárez Chaves, Jefe
Unidad de Tecnologías de la Información (UTI)

ASUNTO: Se somete a valoración de la administración activa, información de los aspectos que deben contemplar las organizaciones (en el presente y futuro), en tiempos de crisis (estado de emergencia); así como comentarios emitidos por esta Auditoría Interna.

Estimados señores:

El 11 de marzo de 2020, la Organización Mundial de la Salud (OMS) declaró oficialmente la pandemia ocasionada por el virus SARS-CoV-2 (COVID-19); momento a partir del cual muchos Gobiernos, de acuerdo con su nivel de afectación, han declarado un estado de emergencia sanitaria y se han visto obligados a replantear su accionar y tomar decisiones sobre una base de incertidumbre, lo que repercute en los diferentes sectores de la economía.

En Costa Rica, el Gobierno de la República a través de las autoridades competentes, ha venido adoptando una serie de lineamientos (restricciones) para minimizar los efectos negativos de la referida pandemia; situación que obliga a los diferentes sectores y ciudadanía en general, a ajustar sus actividades conforme a esas disposiciones; situación de la que no escapa el SFE.

Las Tecnologías de Información y Comunicación (TIC), son herramientas importantes para el cumplimiento de los fines y objetivos de las organizaciones; por cuanto a través de las mismas, se han establecido los soportes y canales mediante los cuales se procesan, almacenan, sintetizan, recuperan y presentan información para soportar la toma de decisiones; por lo que las TIC son transcendentales en el contexto de la atención de emergencias, como es en este caso, la emergencia sanitaria del Covid-19.

La Auditoría Interna desde el año 2009, a través de los servicios de auditoría (estudios) y servicios preventivos (asesorías), ha venido fiscalizando diferentes procesos de la organización; entre ellos, con mayor frecuencia los denominados “Gestión del Control Interno” (su vínculo con la “Gestión de la Calidad”) y “Gestión de la Tecnología de la Información”. Dicha situación ha permitido que la institución adopte medidas para fortalecer su sistema de control interno institucional (SCI).

En el caso de la UTI, la atención efectiva de los productos emitidos por esté órgano de fiscalización, le ha permitido adoptar una serie de medidas para fortalecer el Sistema de Control Interno (SCI) en materia de tecnologías de la información. Entre esas medidas destacan, el cumplimiento del marco de referencia

Martes 12 de mayo, 2020
AI-0122-2020

normativo relacionado con las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) de la Contraloría General de la República y la implementación complementaria, en lo que resulta aplicable, del modelo de gestión internacional de TI denominado "COBIT".

Asimismo, como parte de las regulaciones internas establecidas por la UTI, se encuentra el "Manual de Políticas de Seguridad Tecnología de Información" (TI-M-02) y el "Manual para la recuperación ante desastres (TI-IRS-M-02)"; instrumentos que contribuyen en forma integral a gestionar los diferentes aspectos asociados a las tecnologías de la información (TI).

Si bien tiene claro este órgano de fiscalización que el SFE cuenta con una estructura de control interno que le permite gestionar su actividad; consideramos conveniente compartir y someter a valoración de la administración algunos temas que hemos investigado y que son insumos a considerar por las organizaciones en tiempos de crisis, entre los cuales destacan los siguientes:

- Adopción de un plan y prácticas de respuesta inmediata
- Adopción de medidas con una orientación de futuro
- Fortalecimiento de aspectos asociados a la ciberseguridad (incluye, riesgos asociados)
- Adopción de mejores prácticas con respecto al trabajo remoto

1. SOBRE EL PLAN Y PRÁCTICAS DE RESPUESTA INMEDIATA

A continuación, se describen los aspectos a considerar por las organizaciones para el establecimiento y puesta en marcha de los protocolos que se deben activar ante una emergencia, en los cuales es necesario la participación de las áreas de TI; estos protocolos deben incluir aspectos tales como:

1.1 Planes orientados al establecimiento de una estrategia

Los planes relativos al establecimiento de una estrategia en período de emergencia ("crisis"), deben estar orientados a dar una respuesta inmediata ante los desafíos tácticos, operativos y logísticos; lo anterior es fundamental, por cuanto, una adecuada planificación anticipada estaría contribuyendo a gestionar una ejecución efectiva, dentro de las circunstancias en que se debe operar.

Algunos aspectos esenciales y que deben formar parte de la citada estrategia, están relacionados con la atención de problemas vinculados a mejorar las capacidades de trabajo a distancia y proteger los activos calificados como "sensibles". No obstante, lo primordial es definir una estructura base sobre los diferentes temas relevantes, que deben conformar esa estrategia, entre ellos, se citan lo siguientes:

a) Sobre los planes de continuidad de las operaciones y de recuperación en caso de desastres

En cumplimiento del marco técnico de referencia de TI, las organizaciones como parte de su dinámica, deben contar con planes de continuidad de las operaciones y de recuperación en caso de desastres; por

Martes 12 de mayo, 2020
AI-0122-2020

cuanto de no existir, deben implementarse y de existir, debe evaluarse en forma periódica la capacidad de respuesta y efectividad, documentando y comunicando sus resultados, a las instancias responsables de su análisis, valoración y toma de decisiones.

Sin embargo, ante una emergencia y los efectos de la misma, dichos planes deben revisarse, a efecto de determinar en forma oportuna, que los mismos estén respondiendo a las necesidades de la organización; sobre todo teniendo presente lo siguiente:

- Planes de continuidad: Garantizar en forma razonable que las operaciones se realicen en un ambiente seguro (considera a las personas y lugares de trabajo).
- Planes de recuperación en caso de desastres: Están enfocados a los datos y las aplicaciones.

b) Sobre el equipo de trabajo que operará en la gestión de emergencia

Se debe oficializar el equipo de trabajo que en forma virtual (y excepcionalmente en forma presencial), gestionará la emergencia; el cual debe estar integrado por personal clave, incluyendo al personal de TI, por cuanto el abordaje de la emergencia debe realizarse de forma integral y dependiendo de la naturaleza de cada organización, desde un enfoque multidisciplinario.

c) Sobre el plan de comunicación

El propósito del plan de comunicación está orientado a comunicar lo bueno y lo malo del resultado que se genera producto de la emergencia; el mismo debe considerar, según el contexto de la actividad de la organización, como mínimo, a los siguientes sujetos:

- Empleados
- Proveedores de infraestructura tecnológica, software, etc.
- Usuarios
- Socios comerciales (a nivel nacional e internacional)

Lo anterior, exige la definición de los medios de comunicación mediante los cuales, se divulgará la información de carácter oficial.

d) Sobre la necesidad de validar y/o fortalecer las tecnologías de información

Ante el aviso de una emergencia, así como durante el desarrollo de la misma, se debe analizar oportunamente los diferentes escenarios considerando entre otros aspectos, lo siguiente:

- Disrupciones masivas que se puedan presentar (mano de obra y cadena de suministros –bienes y servicios-).
- Simulación de diversos plazos de respuesta, relacionadas con las actividades claves.

Martes 12 de mayo, 2020
AI-0122-2020

Lo anterior debe permitir, bajo la debida fundamentación técnica, validar los recursos con que se cuenta y/o contemplar la adopción de medidas para fortalecerlos, según las capacidades con las que cuenta la organización.

e) Sobre la necesidad de informar los riesgos reales y/o potenciales

La evaluación de los riesgos y su impacto en la operatividad de la gestión, es un elemento que debe estar presente en la dinámica de toda organización; sin embargo, la gestión de riesgo, en la atención de una emergencia, debe permitir revisar el resultado de riesgos con el que cuenta la organización, a efecto de validarlo y/o ajustarlo, estableciendo como consecuencia, los protocolos necesarios para atenuar y/o evitar la materialización de los mismos.

La información actualizada y asociada a los riesgos reales y/o potenciales dentro del contexto de una emergencia, debe estar al alcance de los funcionarios con la autoridad de tomar decisiones; por cuanto esta debe fluir con precisión y transparencia; el minimizar el efecto de esos riesgos u ocultar los mismos, puede favorecer potencialmente una escalada a riesgos mayores, con las eventuales consecuencias irreparables para la organización.

f) Sobre la identificación de los puestos claves de la organización

La organización debe establecer para cada uno de sus procesos, los puestos clave y el personal sustituto que eventualmente puede asumir esa responsabilidad, ante la ausencia del titular respectivo, lo anterior permitiría mantener la continuidad del servicio ante situaciones adversas generando confianza, tanto en el personal, como en los usuarios y en la ciudadanía en general.

Para lo anterior, se debe garantizar que ese personal clave y sustituto, cuente con el soporte y medios tecnológicos idóneos para el desempeño de sus funciones.

1.2 Prácticas orientadas a la continuidad del negocio

Algunos aspectos que se pueden considerar, a efecto de visualizar prácticas orientadas a la continuidad del negocio, se citan seguidamente:

a) Racionalizar los recursos

Ante una emergencia se debe tener claridad de los diferentes recursos con lo que cuenta la organización, su disponibilidad ante las necesidades emergentes, lo que incluye necesariamente los vinculados con TI. En ese sentido, la alta gerencia es responsable de establecer e implementar los lineamientos que contribuyan con la racionalización de los recursos, definiendo las prioridades respectivas; realizando un monitoreo permanente, a efecto de que la toma de decisiones, se vaya ajustando a los diferentes escenarios que pueden irse presentando, según el comportamiento de la emergencia.

Martes 12 de mayo, 2020
AI-0122-2020

De igual forma, los recursos de TI deben priorizarse para ser destinados en las áreas o procesos críticos para la organización, lo que puede significar inclusive, la modificación del plan anual de trabajo y/o adoptar decisiones respecto a la continuidad, suspensión (total o parcial) o desestimación de proyectos de TI, para re-direccionar esos recursos, conforme al ordenamiento jurídico, en la protección del interés público superior.

b) Ajustar la conectividad, seguridad e infraestructura de TI

Considerando los diferentes escenarios que pueda provocar una emergencia, la organización debe ajustar su marco de acción, a efecto de mantener la continuidad del negocio, situación que obliga a:

- Establecer una modalidad de trabajo a distancia, debiendo contar para ello, con la capacidad tecnológica requerida.
- Contar con demandas de ancho de banda.
- Contar con mecanismos de verificación y accesos.
- Contar con herramientas de seguridad.
- Ajustarse a la aplicación del licenciamiento adquirido; o gestionar la adquisición adicional y/o complementaria necesaria.
- Mantener el monitoreo de la estabilidad de los sistemas, la solidez de la red y la seguridad de los datos; así como gestionar la vulnerabilidad que pueda presentar la infraestructura.

c) Contar con planes de contingencia para el centro de asistencia

El soporte técnico de TI, es un elemento esencial como parte de la dinámica de la organización; sin embargo, en una emergencia, el mismo reviste mayor importancia, por cuanto se deben adoptar las medidas que le permita recibir una demanda mayor a la acostumbrada (ampliar su capacidad instalada) así como definir la priorización de las solicitudes que se presenten, a efecto de tener capacidad de respuesta para atender en forma oportuna, todo aquello vinculado con las áreas críticas y/o prioritarias.

2. SOBRE MEDIDAS CON UNA PROYECCIÓN A FUTURO

Como resultado de la dinámica normal de las organizaciones, es necesario el diagnóstico y evaluación periódica del resultado de la gestión emprendida (trimestral, semestral y anual), a efecto de rendir cuentas y redefinir la forma de hacer las cosas (mejora continua); teniendo como punto clave, la intervención de las tecnologías de la información.

Ante una emergencia, la evaluación de la gestión realizada, durante y después de la misma, debe permitir establecer si las acciones efectuadas deben instaurarse de forma permanente, como parte del sistema de control interno o bien ser ejecutadas únicamente como parte del protocolo de atención de una emergencia respectiva.

Martes 12 de mayo, 2020
AI-0122-2020

Este tipo de proyección a futuro debe analizarse, por cuanto una situación de emergencia genera también oportunidades de mejora, que eventualmente pueden incidir positivamente en la eficiencia, eficacia y economía de las formas de trabajo y protocolos que se lleguen a establecer.

Aspectos que se deben considerar, en el diagnóstico que se realice:

a) Impulsar la automatización de las actividades asociadas a los procesos claves; eliminado rutinas manuales que no tienen razón de ser, situación que obliga, en los casos en que sea requerido, ajustar las regulaciones existentes.
b) Definir y/o fortalecer los lineamientos con respecto a los servicios y la infraestructura en la nube.
c) Consolidar el uso permanente del trabajo virtual, a través del soporte de TI que es requerido; situación que debe fortalecer los mecanismos de supervisión sobre las tareas realizadas, a efecto de garantizar un resultado que responda a los intereses de la organización.

3. SOBRE ASPECTOS ASOCIADOS AL FORTALECIMIENTO DE LA CIBERSEGURIDAD

El crecimiento de las TI, ha sido impulsado a nivel global por la innovación tecnológica, situación que ha permitido el desarrollo positivo en los diferentes sectores de la sociedad.

Se podría indicar que la ciberseguridad representa uno de los desafíos más relevantes de la era digital; por cuanto, entre otros aspectos, está directamente relacionada con la privacidad y protección de datos de las empresas y organizaciones, situación que posibilita hacerle frente a los ciberataques (actos maliciosos contra sistemas de información, infraestructura, redes de comunicación, servidores -bases de datos-, etc.).

En una emergencia, la ciberseguridad debe estar muy presente en las áreas de TI, con el propósito de responder oportunamente ante este tipo de ataques para lo cual es necesario, una adecuada gestión de riesgos sobre esta materia.

Algunos aspectos que se deben considerar:

a) Establecer y/o adaptar las políticas, procesos y actividades de control de ciberseguridad.
b) Fortalecer la gestión de acceso a la identidad.
c) Aumentar en el personal la conciencia ante el surgimiento de nuevas amenazas.
d) Gestionar las conexiones remotas.
e) Contar con un plan de recuperación cibernética.
f) Conocer las amenazas de ciberseguridad vinculadas con los riesgos que enfrentan la organización, así como los trabajadores bajo la figura de trabajo remoto.

4. SOBRE LAS MEJORES PRÁCTICAS CON RESPECTO AL TRABAJO REMOTO

Se procede a describir algunas mejores prácticas relacionadas con el trabajo remoto:

4.1 Establecer previamente los requisitos que todos los trabajadores deben cumplir:

Martes 12 de mayo, 2020
AI-0122-2020

a) Que el perfil del trabajador responda a la automotivación y al ser disciplinado
b) Que su labor la ejerza en atención de una rutina escrita (incluye horarios y pausas)
c) Que cuente con equipo de cómputo requerido
d) Que cuente con conexión a internet requerida
e) Que cuente con acceso a funcionabilidades corporativas, tales como: chat, videoconferencia, llamadas, etc.
f) Que cuente con un espacio dedicado exclusivamente al trabajo (preferiblemente)
g) Que cuente con teléfono (preferiblemente)

4.2 Establecer las acciones que fortalezcan la gestión de la organización, tales como:

a) Gestionar actividades de concientización y capacitación relacionada con la seguridad de la información y ciberseguridad.
b) Ejercer un seguimiento oportuno de accesos sospechosos y situaciones anormales.
c) Priorizar a efecto de garantizar un efectivo acceso remoto seguro.
d) Fortalecer la capacidad de monitorear y analizar la seguridad de la red; así como respecto al uso de datos confidenciales (como ejemplo de ello, correos electrónicos).

5. COMENTARIOS DE LA AUDITORÍA INTERNA

5.1 Lo descrito en la presente comunicación corresponde a una breve reseña de los temas analizados por esta Auditoría Interna respecto al material al que se tuvo acceso; mismo que se somete al conocimiento de la administración como un insumo para su valoración en detalle y una mayor comprensión de las referencias emitidas por este órgano de fiscalización.

5.2 Consecuente con lo anterior, sería conveniente que el SFE, como producto de un diagnóstico de su gestión dentro del marco de la emergencia sanitaria Covid-19, defina el momento oportuno, para establecer el protocolo (estándar) que se activaría en casos de emergencia similares al que se está presentando, como parte del sistema de control interno; lo anterior, claro está, con la flexibilidad necesaria para ajustarse a las circunstancias, dado que cada emergencia debe analizarse en forma particular, atendiendo los lineamientos que emitan las autoridades competentes. En el referido diagnóstico y establecimiento del protocolo correspondiente, se debe considerar la participación permanente de la UTI, por el impacto que su gestión tiene en la continuidad del servicio.

5.3 Es fundamental que la UTI, también realice su propio diagnóstico, con el fin de que documente sus experiencias y resultados generados durante la emergencia sanitaria Covid-19; situación que le permitiría validar y/o ajustar, de ser necesario, su gestión de riesgos, así como sus regulaciones internas e informar lo que corresponda a las instancias pertinentes entre ellas: la Dirección Ejecutiva, Comisión de Control Interno y la Comisión de Tecnologías de la Información.

Martes 12 de mayo, 2020
AI-0122-2020

5.4 Otro aspecto que debe valorar la organización, es conocer la percepción de los funcionarios y usuarios respecto a la gestión emprendida por el SFE (incluyendo el servicio de TI) en el contexto de la emergencia sanitaria Covid-19, para lo cual puede apoyarse, una vez definido el momento oportuno para medir dicha percepción, en la Unidad de Contraloría de Servicios (UCS) y/o Unidad de Planificación, Gestión de la Calidad y Control Interno (PCCI). Este ejercicio podría generar insumos valiosos de análisis para fortalecer el sistema de control interno y según corresponda, cambiar la dinámica institucional, en beneficio de la calidad del servicio y del interés público.

5.5 Como medida para fortalecer la transparencia, rendición de cuentas y la confianza de los usuarios y ciudadanía en general, respecto a la continuidad del servicio en el contexto de la emergencia sanitaria Covid-19, se debe valorar el establecer un medio de comunicación oficial (como podría ser la página web u otros medios), para divulgar los resultados y logros de la gestión institucional.

6. REQUERIMIENTO DE INFORMACIÓN

Se solicita conocer la posición de la **Dirección Ejecutiva y de la Unidad de Tecnologías de la Información (UTI)**, respecto al contenido de la presente comunicación, pero especialmente sobre lo descrito en el numeral 5.

Asimismo, se requiere que la **UTI** informe, **en el marco de la emergencia sanitaria Covid-19**, si ha gestionado lo siguiente:

6.1 Revisión de los riesgos asociados a TI a efecto de validar los riesgos existentes (que están siendo administrados) o bien, ajustar y/o adicionar nuevos eventos de riesgo que deben gestionarse.

6.2 Establecimiento y oficialización de algún tipo de protocolo especial; de ser así, ¿Cuáles han sido los resultados obtenidos de la aplicación de ese protocolo?; ¿cómo se ha venido informando y coordinando con la Dirección?

6.3 Asesoría específica por parte de la Comisión de Tecnologías de la Información a la Dirección del SFE.

6.4 De igual forma, se requiere conocer lo siguiente:

a) ¿Cuál ha sido la experiencia de la aplicación del "Manual para la recuperación ante desastres (TI-IRS-M-02)" durante la gestión que ha venido emprendiendo el SFE en el contexto de la emergencia sanitaria Covid-19?

b) De haberse generado, situaciones relevantes con relación a la aplicación del Manual TI-IRS-M-02, ¿Cuál fue el impacto sobre la operación normal de la organización?

Para la atención del presente requerimiento, se otorga un plazo de **10 días hábiles**.

Atentamente,

HENRY JESUS VALERIN SANDINO (FIRMA)
Firmado digitalmente por HENRY JESUS VALERIN SANDINO (FIRMA)
Fecha: 2020.05.12 14:06:56 -06'00'

Ministerio de Agricultura y Ganadería
Auditoría Interna
Servicio Fitosanitario del Estado

Lic. Henry Valerín Sandino
Auditor Interno

HVS/CQN/IRJ

Nota: Se adjuntan como referencias para la consulta respectiva, los archivos que contienen material emitido por la firma DELOITTE que fue considerado y analizado por la Auditoría Interna:

Anexo 1 - COVID-19 - Nuestros profesionales, la tecnología y el camino a la resiliencia organizacional
Anexo 2 - Respuesta al impacto de la COVID-19 / Respuesta frente a la crisis
Anexo 3 - Liderazgo de Equipos Virtuales Capital Humano - Marzo 2020
Anexo 4 - Cyber Consideraciones de Ciberseguridad en medio de una pandemia global

Ci : *Ing. Leda Madrigal Sandí, Subdirectora*
MBA. Adrián Gómez Díaz, Jefe PCCI
Lic. Alexis Carranza Jiménez, Jefe UCS
Archivo