UNIVERSIDAD DE COSTA RICA

CI Centro de Informática

CONSEJO TÉCNICO ASESOR

Acta de Consejo Asesor CI-41-2021

Celebrada el 04 de agosto de 2021
Aprobada en la sesión No. 49-2021 del 15 de diciembre de 2021

Tabla de Contenido

Acta de la sesión ordinaria número cuarenta y uno, celebrada por el Consejo Técnico Asesor a las nueve horas del día cuatro de agosto de dos mil veintiuno.

Asisten a esta sesión: M.T.I. Henry Lizano Mora, Director Centro de Informática; Máster Tatiana Bermúdez Paéz, Subdirectora; M.T.I. Jorge Vargas Umaña, Coordinador de la Unidad de Riesgos y Seguridad (URS); MAP. Pedro Céspedes Calderón, Coordinador del Área de Desarrollo de Sistemas y del Área de Captación y Promoción (ACP); M.A.U. Ana Yanci Tosso Marín, Coordinadora de la Unidad Administrativa y de Recurso (UAR); M.Sc. Abel Brenes Arce, Coordinador del Área de Investigación y Desarrollo (AID); M.Sc. Rebeca Esquivel Flores, Coordinadora del Área de Gestión de Comunicaciones (AGC); Ing. Wilfredo Fonseca Vargas, Coordinador del Área de Gestión de Servicios (AGS); Lic. Jairo Sosa Mesén, Coordinador del Área de Gestión de Usuario (AGU); Bach. Jorge Carranza Chavez, Coordinador del Área de Gestión de Infraestructura (AGI); Licda. Heylin Pacheco Rodríguez, Coordinadora Unidad de Calidad y Mejora Continua (UCM) y Bach. Cindy Arias Quiel, Coordinadora de la Unidad de Gestión de Adquisiciones (UGA).

La sesión inicia a las nueve horas con trece minutos con la presencia de los siguientes miembros: M.T.I. Henry Lizano Mora, M.T.I. Jorge Vargas Umaña, MAP. Pedro Céspedes Calderón, M.Sc. Abel Brenes Arce, M.Sc. Rebeca Esquivel Flores, Ing. Wilfredo Fonseca Vargas, Lic. Jairo Sosa Mesén, Bach. Jorge Carranza Chavez, Licda. Heylin Pacheco Rodríguez y Bach. Cindy Arias Quiel.

Ausentes con justificación: Máster Tatiana Bermúdez Paéz y M.A.U. Ana Yanci Tosso Marín.

El M.T.I. Henry Lizano Mora, Director del Centro de Informática, da lectura al orden del día:

1. Orden del día
2. Presentación de propuesta para definir el equipo de incidencias, a cargo del señor Jorge Vargas.
3. Uso y acceso a los cuartos de comunicación, a cargo del señor Jorge Carranza.
4. Auditoría Externa de TI 2020, a cargo de la señorita Heylin Pacheco.
5. Informe del estado de compras de 2021 y datos importantes para cada proceso, a cargo de la señora Cindy Arias.
6. Varios

Artículo 1. ***Presentación de propuesta para definir el equipo de incidencias, a cargo del señor Jorge Vargas.***

El señor Jorge Vargas comenta que la Unidad de Riesgos y Seguridad (URS), en conjunto con la Unidad de Calidad y Mejora Continua (UCM), plantearon un procedimiento apoyado con instrumentos (formularios) para llevar un control como historial de los incidentes de seguridad. Además, el señor Abel Brenes más adelante procederá a mostrarles la propuesta de la parte tecnológica. Indica que dicho procedimiento fue compartido al coordinador del Área de Gestión de Usuarios (AGU), como actor clave en la atención de los incidentes de seguridad, ya que esta Área tiene relación directa con los usuarios.

El Sr. Vargas procede a mostrar el procedimiento a los miembros del Consejo Técnico Asesor, el cual se encuentra adjunto en esta acta como Anexo 1.

Indica que este proceso comprende la ejecución de actividades que deben llevarse a cabo ante la ocurrencia de incidentes de seguridad, de acuerdo con las siguientes etapas:

1. **Levantar el incidente de seguridad de la información:** ante la ocurrencia de un incidente de seguridad, se debe completar el formulario "*CI-URS-F11 Reporte de incidentes de seguridad de la información*", el cual deberá remitirse al correo incidentesseguridad@ucr.ac.cr. Una vez recibido el formulario, el coordinador de AGU, se comunica con la persona que lo realizó para indicarle que el incidente está siendo atendido.

2. **Categorizar el incidente de seguridad:** el coordinador de URS verifica si el incidente de seguridad se califica como uno de seguridad o no.

3. **Escalar el incidente de seguridad:** el coordinador de URS realizará el análisis preliminar para determinar el nivel de afectación, alcance, pronóstico de expansión y los daños potenciales o reales que se generen, así como las posibles acciones de mitigación que correspondan y la priorización de atención del evento. Convoca a las coordinaciones involucradas y al equipo de respuesta que va a apoyar a la solución.

4. **Investigar el incidente de seguridad:** la coordinación del área definida realiza un estudio preliminar del tipo de incidente.

5. **Solucionar el incidente de seguridad:** la coordinación del área definida asigna a un funcionario experto del área como responsable de llevar la trazabilidad de atención del evento y, en conjunto con el equipo de respuesta, se valoran y aplican las actividades de solución que se consideren adecuadas para resolver el incidente y prevenir que ocurra en el futuro.

6. **Recuperar:** la coordinación del área definida supervisa que el equipo de respuesta ejecute las actividades de recuperación asociadas al tipo de incidente presentado, de acuerdo con los procedimientos documentados existentes o mediante la implementación de otras actividades.

7. **Cerrar los incidentes de seguridad:** la coordinación del área definida documenta en el formulario *CI-URS-F12 "Atención de Incidentes de Seguridad de la Información"*, las acciones realizadas en la atención del mismo y lo remite a las coordinaciones de AGU y URS. Posteriormente, el coordinador de AGU se comunica con el gestor de TIC que reportó el incidente para dar por atendido el mismo y el coordinador de URS documenta en el consecutivo *CI-UCR-C01 Consecutivo de Incidentes de Seguridad de la información* la hoja "*Atención*" y se presenta al director del CI el informe correspondiente.

Al respecto, el señor Jorge Vargas aclara que en la primera etapa, la persona que llena el formulario es el funcionario del CI que recibe la alerta y no la persona que la reporta.

La señora Heylin Pacheco comenta que respecto a la aprobación de este procedimiento y sus formularios, se hará un ejercicio con un evento que sucedió en el pasado y un evento nuevo, con el fin de analizar cómo fluye el proceso y verificar si deben hacerse mejoras.

El señor Abel Brenes presenta una propuesta para el *Centro de operación y monitoreo de servicios.*

Al respecto, el Sr. Brenes procede a mostrar la estructura de soporte de un Centro de Operaciones de Red (NOC), el cual es una ubicación desde donde se monitorean, mantienen y supervisan las redes y servicios TIC.

Comenta que los servicios del NOC detectan, diagnostican y solucionan problemas en cuatro áreas: servidores, redes, aplicaciones y sitios web.

Los ejes del NOC son:

- Organización.
- Automatización de procesos.
- Aprovisionamiento.
- 24x7
- Monitoreo 3 capas
- ItasS: el futuro.

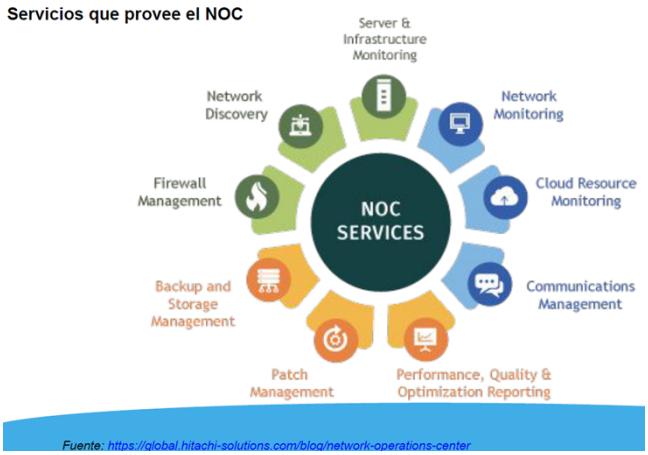
Además, el señor Abel Brenes indica que los servicios de NOC incluyen:

- Instalar, solucionar problemas y actualizar aplicaciones de software – Administrar servicios de correo electrónico.
- Gestionar el almacenamiento y la copia de seguridad de datos.
- Realizar evaluaciones de red y descubrimiento de activos.
- Hacer cumplir las políticas de la red de TI.
- Generar informes de rendimiento y recomendaciones para mejoras.
- Supervise los cortafuegos y los sistemas de prevención de intrusiones.
- Realice análisis y reparación antivirus. Análisis de amenazas.

El señor Abel Brenes hace una comparación entre el Help Desk y la NOC, e indica que el Help desk es el que atiende a los usuarios y que recibe, de parte de los diferentes usuarios, elementos de soporte, pero existen niveles, a éste no se le puede pedir especialización, para esto está el NOC, en donde se encuentran las personas que tienen el control especializado a un nivel mayor.

Posteriormente, muestra los servicios que provee el NOC, según se detalla en la siguiente

imagen:



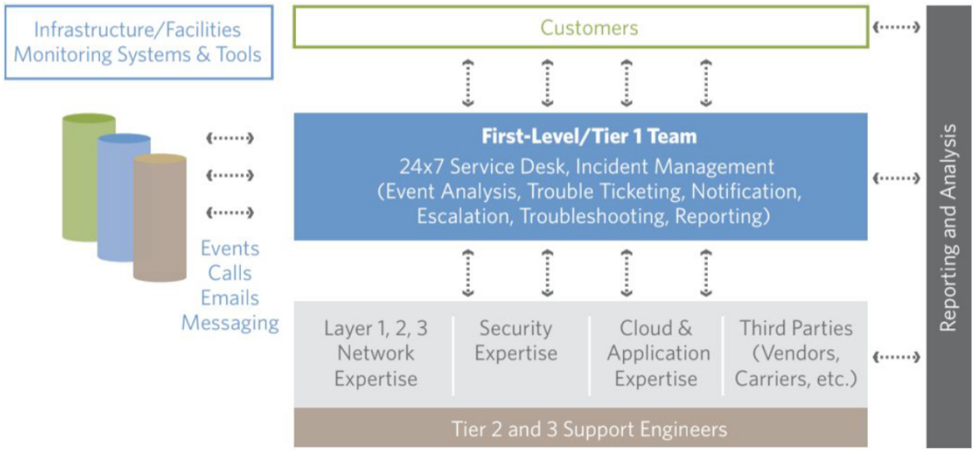
Con esto se busca la mitigación de efectos negativos a través del NOC, según se muestra en la siguiente imagen:

Por otro lado, el señor Abel Brenes indica que el NOC tiene roles especializados y que no únicamente están los ingenieros, sino también los líderes de equipo y analistas de triage.

El señor Abel Brenes comenta que un NOC exitoso es aquel que redirecciona adecuadamente el tiquete.

Además, muestra la estructura de soporte de un Centro de Operaciones de Red (NOC), según se detalla a continuación:

Estructura de soporte de un Centro de operaciones de Red (NOC)

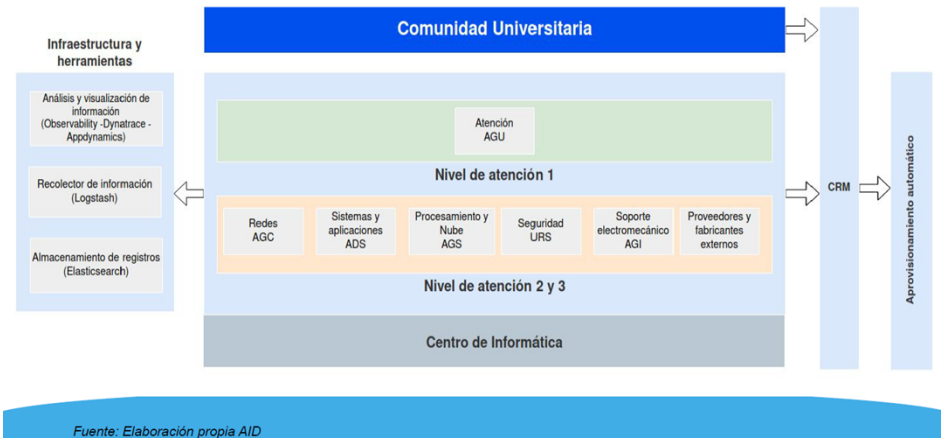


Fuente: https://www.inoc.com/blog/noc-best-practices-10-ways-to-improve-your-operation

Se retira la señora Heylin Pacheco a las diez horas con doce minutos.

Posteriormente, el Sr. Brenes muestra un mapeo de la estructura de soporte de un Centro de Operaciones de Red (NOC) en el Centro de Informática, según se detalla a continuación:

Mapeo C.I. del soporte de un Centro de operaciones de Red (NOC)

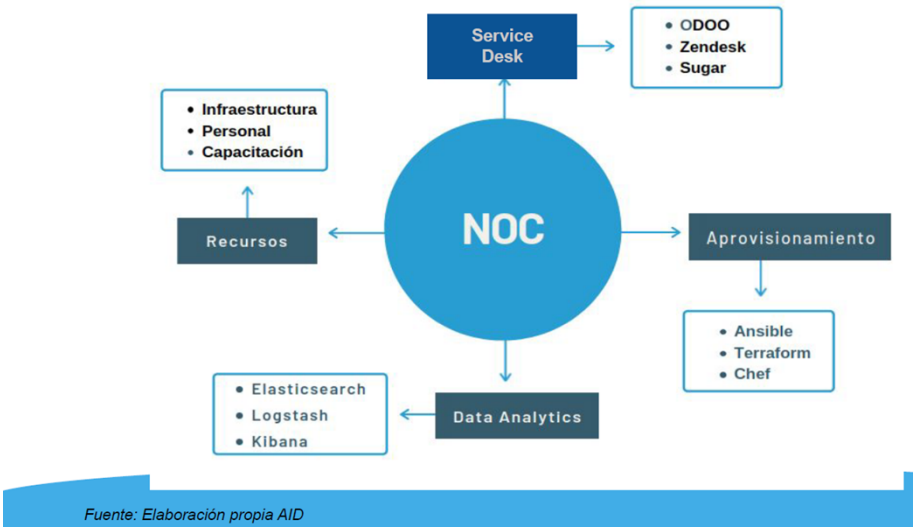


Fuente: Elaboración propia AID

Ingresa la señora Heylin Pacheco a las diez horas con catorce minutos.

Posteriormente, detalla las herramientas de apoyo y soporte del NOC:

Herramientas de apoyo y soporte de un Centro de operaciones de Red (NOC)



Fuente: Elaboración propia AID

Comenta que todo esto está basado en el IT como Servicio (ItaaS) que:

- Mejora la eficiencia en la construcción, organización e implementación de servicios simples o compuestos.
- Automatiza el cumplimiento mediante la aplicación de políticas de control de acceso y seguridad.
- Cumplimiento de autoservicio para los usuarios por servicios externos e internos.
- Se integra con los sistemas internos de TI y los procesos organizativos.
- Servicios y plataformas alertas proactivamente.

El señor Pedro Céspedes consulta si este servicio se puede tercerizar, a lo que el señor Abel Brenes indica que todo se puede tercerizar, a lo que el Sr. Céspedes considera que el acceso es muy delicado para terciarizarlo. Al respecto, el señor Henry Lizano indica que esto debe evaluarse en razón de costo – beneficio y que hay otras entidades que ya lo están utilizando.

Por otra parte, el señor Jairo Sosa indica que no le queda clara cuál era la propuesta o si más bien esta presentación era informativa para conocer lo que era el NOC, a lo que el señor Abel Brenes indica que el objetivo de la presentación era para tener una visión general de lo que es un NOC, mostrarles como se mapeaba inhouse, pero con todas las

limitaciones de que no se puede operar 24/7 y por último mostrar la ruta que el señor Henry Lizano ha venido impulsando de utilizar el leasing como un modelo para viabilizar las operaciones.

Se retira el señor Henry Lizano a las diez horas con veintitrés minutos.

El señor Abel Brenes comenta que es una forma de hacer un alquiler sumando servicios de un socio de negocios que pueda manifestarse.

Ingresa el señor Henry Lizano a las diez horas con veinticuatro minutos.

La señora Rebeca Esquivel comenta que ya el Centro de Informática cuenta con un NOC en el que las alertas llegan en tiempo real, pero el problema complejo siempre ha sido la disponibilidad, por lo que considera importante valorar invertir en los profesionales que ya tiene el CI, porque realmente el sistema de monitoreo con el que se cuenta es muy bueno.

El Sr. Lizano indica estar de acuerdo con la señora Rebeca Esquivel, sin embargo, considera importante que se tengan datos para realizar una comparativa y así tomar la mejor decisión, porque se requiere un servicio 24/7.

Al respecto, el señor Wilfredo Fonseca comenta que a final de cuenta el NOC es la operatización del concepto de TI como servicio. Indica que está de acuerdo con lo indicado por la señora Rebeca Esquivel, pero que a pesar de que se cuenta con una plataforma, se le tiene que dar mantenimiento, soporte y atender incidentes sobre la plataforma que monitorea y que más bien ésta debería ser un apoyo para que las personas se integren a actividades que generen más valor, por lo que considera que el cambio de paradigma es importante.

El señor Abel Brenes indica que la idea es mostrar que hay una organización del NOC que no existe en el CI, ya que no se cuenta con: monitoreo de tres capas, automatización de procesos, ni operaciones 24/7, por lo que en ese sentido es valido indicar que IT como servicio es el futuro y el tema de las nuevas adquisiciones vendrán como ese modelo de leasing o servicios administrados.

Acuerdo 1.1: Se acuerda aprobar el *Procedimiento para la Gestión de Incidentes de Seguridad de la Información,* presentado por el señor Jorge Vargas, con el fin de que sea divulgado e implementado. **Acuerdo con diez votos a favor y ninguno en contra en el momento de la votación. ACUERDO EN FIRME.**

El señor Jorge Vargas consulta si respecto al service desk y el NOC, se propone a alguien para que trabaje en el diseño, a lo que el señor Henry Lizano propone que se conforme una comisión para el trabajo en conjunto del diseño del service desk, para lo cual solicita al señor Abel Brenes iniciar con el diseño e incorpore, durante el proceso, a las diferentes áreas y se conforme un equipo de trabajo en conjunto con el señor Jairo Sosa y la señorita Heylin Pacheco.

El señor Henry Lizano realiza un receso a las diez horas con cuarenta y ocho minutos.

Se reanuda la sesión a las once horas con cuatro minutos.

Artículo 2: Uso y acceso a los cuartos de comunicación, a cargo del señor Jorge Carranza.

El señor Jorge Carranza comenta que se han recibido solicitudes, por parte de directores de unidades y de RIDs, para que el CI les otorgue copia de las llaves de acceso a los cuartos de comunicación. Sin embargo, optó por traer este tema ante el Consejo Técnico Asesor, ya que es un tema bastante delicado.

Al respecto, comenta que existe un lineamiento para el uso y manejo de las llaves, pero el mismo debe actualizarse, ya que no es acorde a lo que se tiene ahorita.

El señor Henry Lizano comenta que algunas de estas solicitudes están justificadas, sin embargo, el principal problema es que personal del CI se debe estar desplazando al sitio para abrir los cuartos de comunicación, por lo que la propuesta sería cómo abordar estas excepciones.

La señora Rebeca Esquivel indica que se podría evaluar un proyecto de préstamo de llave, a excepción de los MDF, ya que en algunas construcciones se ha dado el robo de cables, racks y otros. Considera que se puede establecer un procedimiento de acceso a los cuartos de comunicación. Sin embargo, el señor Jorge Carranza indica que el problema es que la llave es la misma para los MDF. A su vez, la Sra. Esquivel comenta que la ventaja es que la mayoría de los MDF tienen cámara.

El señor Jorge Carranza indica que una opción válida es solicitar a un cerrajero realizar una llave distinta para ingresar a los cuartos de comunicación, así no habría que darle la llave maestra, pero esto tendría una implicación económica. Al respecto, el señor Henry Lizano señala que esta es una buena opción y que los gastos por concepto de copias de llaves podrían cargarse a la unidad contable 878 o a la unidad contable 899 de la CIEQ y que en caso que no se cuente con suficiente presupuesto se podría valorar con la unidad interesada.

El señor Abel Brenes comenta que hace unos años atrás se planteó un proyecto de hacer cerraduras electrónicas, mediante llaves codificadas, por lo que considera que este proyecto sería muy interesante revisarlo y valorarlo. Este proyecto ya había sido escrito y costeado, por lo que considera importante se pueda retomar.

El señor Lizano solicita valorar todas las opciones que se tengan y a la vez solicita revisar los lineamientos existentes al respecto y sino hacer la consulta ante la Oficina Jurídica.

Por su parte, el señor Wilfredo Fonseca indica que se debe buscar la manera de como

sentar responsabilidades, independientemente de la forma que se use para ingresar, esto con el fin de evitar que se presenten situaciones como hurtos o robos, a lo que el señor Henry Lizano comenta que se debe crear un documento de descargo de responsabilidades con todos los alcances que esto implique, por lo que solicita al señor Jorge Carranza en conjunto con la señora Heylin Pacheco crear este documento. Además, solicita al Sr. Carranza presentar una actualización de este tema en el próximo Consejo Asesor.

Artículo 3: Auditoría Externa de TI 2020, a cargo de la señorita Heylin Pacheco.

La señora Heylin Pacheco comenta que se presenta este tema ante el Consejo con el fin de ponerlos en contexto y tratar de llegar a un acuerdo sobre el tiempo que requieren para realizar la retroalimentación de los hallazgos.

Comenta que a inicios de año, se pronunciaron sobre el avance en la atención de los hallazgos de la Auditoría Externa del 2019. Posteriormente, llegó el informe de auditoría 2020, se recolectaron los requerimientos y se va a dar un seguimiento integral, no sólo a nivel del CI sino a nivel institucional y comenta que el señor Jesús Brenes estará recopilando e integrando la información.

Además indica que algunos coordinadores deberán atender hallazgos a nivel institucional, por lo que se deberán buscar soluciones integrales. Indica que en esta solución integral, se tiene como fecha límite el 30 de noviembre de 2021, comenta que ya se tiene una hoja de cálculo con todos los hallazgos y procede a consultarles cuanto tiempo requieren para buscar la solución con acciones y fechas. Indica que debe tomar en cuenta que la dirección debe revisarlo y luego devolverlo para ajustes y posteriormente se enviarán a la Rectoría a finales de noviembre.

El señor Jorge Vagas propone que la señorita Heylin Pacheco les envíe la solicitud a los coordinadores los hallazgos mediante una Validación Técnica.

Artículo 4: Informe del estado de compras de 2021 y datos importantes para cada proceso, a cargo de la señora Cindy Arias.

La señora Cindy Arias comenta que anteriormente les compartió por correo electrónico un documento con los requisitos de los procesos de compra, sin embargo, a la vista de que se tienen nuevas coordinaciones, trajo este tema ante el Consejo para refrescar algunos procedimientos.

Al respecto menciona que los procesos de apertura tienen que ser mínimo de tres días y posteriormente se debe dar tiempo para las aclaraciones, si requieren un proceso de apertura de 24 horas, este debe justificarse e incluirse en SICOP.

La señora Cindy Arias procede a mostrar los requisitos mínimos documentales por tipo de compra, el cual se adjunta a esta Acta como Anexo #2. Además, comenta que este

documento se los compartió ayer por la noche.

El señor Henry Lizano agradece a la señora Cindy Arias el documento compartido ya que la información es bastante clara.

Posteriormente, la señora Cindy Arias muestra una tabla de contrataciones 2021 en la que se detalla toda la información de los diferentes procesos de compras que tramita la Unidad de Gestión de Adquisiciones (UGA). Indica que es importante que los coordinadores le den seguimiento a esta información y que si requieren algún código se lo pueden pedir a ella o a cualquier compañero de UGA.

Asimismo, indica que el señor Freddy Díaz, de la oficina de presupuesto, les indicó que el barrido presupuestario se realiza este mes, por lo que solicita que todo lo que tengan pendiente lo pasen a UGA cuanto antes para darle prioridad en GECO. Además, queda atenta en caso de que tengan alguna duda o consulta e informa que está en la mejor disposición de colaborar.

El señor Henry Lizano comparte un correo enviado por la señora Patricia Vásquez, sobre compras pendientes en la unidad contable 878 y detalla cada una de ellas. Al respecto, la señora Cindy Arias comenta que de esas compras sólo está pendiente la renovación del contrato de mantenimiento de los blades.

Artículo 5: Varios.

- ➢ El señor Jorge Vargas informa que el plan de continuidad de todas las plataformas del Área de Gestión de Infraestructura (AGI) ya se completó. El informe final consta de 56 páginas y está debidamente firmado por la Unidad de Riesgos y Seguridad (URS) y AGI. Indica que esto es digno de celebrar y agradece a los señores Jorge Carranza, Gustavo Quirós y a todo el equipo de AGI, que se pusieron a la orden y se logró cumplir con todo el plan de continuidad y los planes de contingencia y mitigación, para asegurar al máximo posible toda la gestión de infraestructura. Además, menciona que le darán seguimiento de forma semestral con el fin de verificar su cumplimiento. Al respecto, el señor Henry Lizano solicita a la señora Melissa Cerdas, coordinar una reunión con los señores Jorge Carranza y Jorge Vargas, para que le presenten dicho informe.

- ➢ El señor Jorge Vargas informa que respecto al análisis de vulnerabilidades que están haciendo a los servidores virtuales, se han enviado tres informes a todos los gestores de TI que tienen servidores virtuales en el CI e indica que llevan un pulso de la atención de éstos. Comenta que ya tienen gente en rojo que no ha atendido las vulnerabilidades críticas y menciona que esta semana entregarán el cuarto informe y, que según la respuesta que se tenga, se tomarán acciones con respecto a su atención. Indica que la propuesta es que los coordinadores le propongan como abordar esos análisis de vulnerabilidades sobre las plataformas que gestionan.

- ➢ El señor Jairo Sosa consulta, si respecto a este tema que menciona el señor Jorge

Vargas, si se están tomando en cuenta los tiquetes que se han generado y que no han sido posibles atender, debido a la cantidad de personal con que cuenta el Área de Gestión de Usuarios (AGU). Por lo que es importante tenerlo en consideración, ya que diferentes unidades han solicitado colaboración mediante tiquete, sin embargo, se les está brindando la colaboración a un paso lento. A lo que el señor Henry Lizano, indica que el interesado debe utilizar, dicha solicitud, como evidencia para indicar que está en proceso.

➢ El señor Henry Lizano recuerda que todo proceso o procedimiento nuevo que se cree, debe ser validado por la Unidad de Calidad y Mejora Continua (UCM), con el fin de tener el control documental correspondiente, por lo que solicita que se involucre a ésta en la creación del documento.

Se levanta la sesión a las doce horas con quince minutos.

UCR Firmado digitalmente

M.T.I. Henry Lizano Mora
Director

MCG

ANEXOS

Anexo #1

Registro de documentos antecedentes

Sesión 41-2021 ordinaria

04 de agosto de 2021

No. Artículo	Documento	Fecha
1	Procedimiento para la gestión de incidentes de seguridad de la información	20-07-2021
4	Requisitos documentales 2021	27-04-2021