ACTA N° 059-2022 ***24 DE NOVIEMBRE DEL 2.022***

SESIÓN ORDINARIA

ORDEN DEL DÍA

CAPITULO I		***ASUNTOS PRELIMINARES.***
	ARTÍCULO 1.-	***VERIFICACIÓN QUORUM.***
	ARTÍCULO 2.-	***APROBACIÓN DEL ORDEN DEL DÍA.***
CAPITULO II		***TEMAS PROPIOS DE LA JUNTA DIRECTIVA.***
	ARTÍCULO 3.-	***REVISIÓN visión y aprobación de actas anteriores 037-2022 y 038-2022.***
CAPITULO III		***INFORMES DE LA ADMINISTRACIÓN.***
	ARTÍCULO 4-	***INFORME Y JURAMENTACIÓN DE MIEMBROS DE LA JUNTA DE RELACIONES LABORALES DE JASEC.***
	ARTÍCULO 5.-	***INFORME SOBRE CIBERATAQUE A LA INFRAESTRUCTURA TECNOLÓGICA DE JASEC ABRIL 2022.***
CAPITULO IV		***OTROS ASUNTOS.***
	ARTÍCULO 6.-	***ASUNTOS VARIOS.***

……

……

……

……

……

……

……

……

……FIRMA DEL ACTA……

ACTA 059-2022

Sesión ordinaria celebrada por la Junta Administrativa del Servicio Eléctrico Municipal de Cartago. **VERIFICACIÓN DE QUÓRUM:** Al ser las veinte horas del día jueves veinticuatro de noviembre del año dos mil veintidós, están presentes en el salón de sesiones a través de la plataforma virtual webex, los directores, Lizandro Brenes Castillo, quien preside, Anelena Sabater Castro, Secretaria, Rita Arce Láscarez, Rosario Espinoza Carazo, y Ana Lía Solano Pacheco. **INICIO DE LA SESIÓN:** Se cuenta con el quórum reglamentario para la celebración de la sesión. **INGRESO DE LOS DEMÁS DIRECTORES:** Al ser las dieciocho horas con doce minutos, ingresó el director Salvador Padilla Villanueva. Al ser las dieciocho horas con trece minutos, ingresó el director Alexander Mejías Zamora, Vicepresidente. Además, participan los señores: Francisco Calvo Solano, Gerente General, Juan Antonio Solano Ramírez, Asesor Jurídico, María Celina Madrigal Lizano, Auditora Interna, Georgina Castillo Vega, Profesional de Junta Directiva…..

CAPITULO I		***ASUNTOS PRELIMINARES.***

ARTÍCULO 1.- VERIFICACIÓN QUÓRUM.

Se da inicio a la sesión con el quórum respectivo……..……

ARTÍCULO 2.- APROBACIÓN DEL ORDEN DEL DÍA.

Presenta don Lizandro Brenes la propuesta de Orden del Día, según el siguiente detalle:…….

CAPITULO I		***ASUNTOS PRELIMINARES.***
	ARTÍCULO 1.-	***VERIFICACIÓN QUÓRUM DE LA SESIÓN.***
	ARTÍCULO 2.-	***APROBACIÓN DEL ORDEN DEL DÍA.***
CAPITULO II		***TEMAS PROPIOS DE LA JUNTA DIRECTIVA.***
	ARTÍCULO 3.-	***REVISIÓN Y APROBACIÓN DE ACTAS ANTERIORES Nº 037-2022 y 038-2022.***
CAPÍTULO III		***INFORMES DE LA ADMINISTRACIÓN.***

	ARTÍCULO 4.-	***INFORME Y JURAMENTACIÓN DE MIEMBROS DE LA JUNTA DE RELACIONES LABORALES DE JASEC. (Tiempo: 15 min presentación y 10 min. discusión)***
	ARTÍCULO 5.-	***INFORME SOBRE CIBERATAQUE A LA INFRAESTRUCTURA TECNOLÓGICA DE JASEC ABRIL 2022. (Tiempo: 60 min presentación y 30 min. discusión)***
CAPITULO IV		***OTROS ASUNTOS.***

Somete don Lizandro Brenes a discusión el orden del día……

Externa el señor Brenes Castillo: los que estén a favor de aprobar el orden del día sírvanse por favor; tenemos entonces 5 votos, queda aprobado el orden del día……..

SE ACUERDA: de manera unánime y afirmativa, con cinco votos presentes……

2.a.- Aprobar el orden del día presentado por la Presidencia de la Junta Directiva para la sesión Nº 059-2022……

Externa don Lizandro Brenes: para que doña Anelena (Sabater) tome nota que doña Rita Arce no está en la sesión virtual, pero sí está en la sesión presencial, y que ella votó a favor, para que por favor conste en actas que ella levantó la mano a nivel presencial a la vista de todos…….

Resalta doña Anelena Sabater: correcto, consta……...

CAPITULO II		***TEMAS PROPIOS DE LA JUNTA DIRECTIVA.***

ARTÍCULO 3.- REVISIÓN Y APROBACIÓN DE ACTAS ANTERIORES 037-2022 Y 038-2022.

Somete la Presidencia a discusión el acta Nº 037-2022……...

Somete don Lizandro Brenes a votación la aprobación del acta Nº 037-2022……..

Vota doña Rita Arce a favor……..

Vota don Lizandro Brenes a favor……

Vota doña Rosario Espinoza abstención…….

Vota don Alexander Mejías abstención ……..

Vota don Salvador Padilla abstención ……

Vota doña Anelena Sabater abstención …….

Vota doña Analía Solano abstención…..……..

SE ACUERDA: de manera afirmativa, con dos votos de los directores Arce Láscarez y Brenes Castillo y la abstención de los directores Espinoza Carazo, Mejías Zamora, Padilla Villanueva, Sabater Castro y Solano Pacheco……..

3.a. Aprobar del acta de las sesión Nº 037-2022…….……..

Somete la Presidencia a discusión el acta Nº 038-2022……...

Somete don Lizandro Brenes a votación la aprobación del acta Nº 038-2022……..

Vota doña Rita Arce a favor……..

Vota don Lizandro Brenes a favor……

Vota doña Rosario Espinoza abstención…..……

Vota don Alexander Mejías abstención ……..

Vota don Salvador Padilla abstención ……

Vota doña Anelena Sabater abstención …….

Vota doña Analía Solano abstención…..……..

SE ACUERDA: de manera afirmativa, con dos votos de los directores Arce Láscarez y Brenes Castillo y la abstención de los directores Espinoza Carazo, Mejías Zamora, Padilla Villanueva, Sabater Castro y Solano Pacheco……..

3.b. Aprobar el acta de la sesión Nº 038-2022……..

CAPITULO III		***INFORMES DE LA ADMINISTRACIÓN.***

ARTÍCULO 4.- INFORME Y JURAMENTACIÓN DE MIEMBROS DE LA JUNTA DE RELACIONES LABORALES DE JASEC.

Se conocen los siguientes documentos: 1. Oficio Nº GG-859-2022 suscrito por el Lic. Francisco Calvo Solano, Gerente General; 2. Oficio Nº SUBG-TH-0798-2022, suscrito por el Lic. Arnold Mora Muñoz,

Jefe a.i. Departamento Talento Humano y Licda. Magaly Cáseres Madrigal, Profesional Nivel 2 Talento Humano; 3. Presentación Elecciones JRL; 4. Oficio Nº GG-858-2022 suscrito por el Lic. Francisco Calvo Solano, Gerente General……..

Para este punto se encuentra presente el Lic. Arnold Mora Muñoz, Jefe a.i. Departamento Talento Humano, quien mediante diapositivas presentará este informe……..

Inicia don Arnold Mora indicando que: en el caso de JASEC tenemos la figura de la Junta de Relaciones Laborales que está establecido en la Convención Colectiva, en este caso procedimos a hacer el proceso de elección de los representantes de los trabajadores ante la Junta de Relaciones Laborales para que estén debidamente nombrados por un periodo de 3 años que es lo que establece la Convención Colectiva, generalmente está Junta lo que hace es revisar los informes de los órganos directores de procedimiento administrativo, y emiten un dictamen de previo a que el órgano decisor emita el respectivo acto final, esa es como la principal función que dicha Junta ha tenido desde que se ha conformado, igual pueden hacer temas de interpretación de la Convención Colectiva como tal, y cualquier aspecto relacionado precisamente con las relaciones laborales a nivel interno. Entonces bueno, para este año se tenía el vencimiento de los representantes de los trabajadores, y en el caso de Talento Humano realizó el proceso de elecciones de acuerdo con lo que está establecido en el reglamento……

Continúa el señor Mora Muñoz indicando: nosotros trabajamos bajo un cronograma de trabajo, que es el que nos va guiando con todas las actividades que hay que realizar, desde el momento en que se hace la convocatoria a nivel institucional, hasta propiamente el momento en que se realiza la juramentación de las personas que hayan sido seleccionadas o que hayan quedado electas, en este caso en ese cronograma nosotros definimos las fechas, como les digo se hacen diferentes comunicados a nivel interno, y se realiza propiamente el proceso de elecciones, en primera instancia, digámoslo así la primer ronda se realizó el día 8 de noviembre que fue la fecha que establecimos para efecto de cumplir con los tiempos que establece el mismo reglamento de la Junta de Relaciones Laborales……..

……..

ACTIVIDAD	FECHAS DE CUMPLIMIENTO	RESPONSABLE
Convocatoria a las elecciones	07 de octubre del 2022	Departamento Talento Humano
Fecha límite para recibir postulaciones	Del 07/10/2022 al 11/10/2022	Funcionarios interesados
Comunicación de Postulaciones	12 de octubre del 2022	Departamento Talento Humano
Campaña promocional de Postulantes	Del 12 de octubre al 07 de noviembre del 2022	Papeletas Postulantes
VOTACIONES	**08 de noviembre del 2022**	**Todos los funcionarios empadronados**
Declaratoria de los resultados de las votaciones	09 de noviembre del 2022	Tribunal Electoral al Departamento Talento Humano
Comunicación de los resultados de las votaciones y elaboración de Informe sobre resultados	09 de noviembre del 2022	Departamento Talento Humano
Juramentación de la Junta Directiva del FRL	11 de noviembre del 2022	Junta Directiva de JASEC

Fuente: SUBG-TH-C-010-2022

Hace ver don Arnold Mora que: es importante mencionar que a nivel de elecciones se conforma un tribunal electoral que está conformado por representantes de cada uno de los centros de trabajo, cuya función principal es velar que durante el día las elecciones el proceso transcurra sin ningún inconveniente, incluso también para ayudarle a los compañeros a ejercer el voto, principalmente porque desde que estamos con el tema de la pandemia se instauró una modalidad virtual, de previo lo hacíamos con un modelo tradicional el cual era con la papeleta en físico y cada quien emitía su voto, pero por el tema la pandemia se desarrolló una aplicación a nivel interno que es la que hemos estado utilizando para estos procesos de elección, entonces ahí está el detalle de los compañeros que conformaron el tribunal, se nombra a una Presidenta que es la que finalmente emite el informe final, de acuerdo con los resultados que cada uno envía al final del día con las elecciones……

Nombre Funcionario	Centro
Sergio Picado Granados	Tuis
Amado Vega Fernandez / Álvaro Josué Fernández Arrieta	Barro Morado
Fabio Castillo Calderón / Keylin Araya Sandoval	Birris
Jason Del Valle Flores / Loaiza Valerin Mauricio	El Bosque
Guiselle Monge Leitón	Sede Central
Sheyla Alvarado Jimenez	
Inés Martinez Leandro	Barrio Fátima
María José Rodríguez Conrado (Presidente del Tribunal)	Infocomunicaciones

Comenta don Arnold Mora que: las pantallitas que están ahí en la presentación es como el paso a paso que cada persona tiene que seguir a la hora de ejercer el voto, repito que es una aplicación virtual, es un enlace que se habilita para que los compañeros se logueen con su usuario y con la respectiva contraseña que cada uno tiene, para que eso sea con un filtro de control y seguridad, en ese sentido como parte del proceso que la persona tiene que realizar es que tiene que escoger el centro de trabajo en el cual está ejerciendo el voto, para que eso ayuda a los compañeros del tribunal a cuantificar el tema de las papeletas y los votos emitidos, en la tercer pantalla se muestra la imagen que a cada uno le despliega con el detalle precisamente de las papeletas que están participando, en este caso tuvimos la particularidad de que fue solo una papeleta, entonces ahí se detalla el nombre de las compañeras en este caso, y también el tema de voto en blanco y voto nulo, una vez que la persona ya ejerce el voto y marca con una “x”, ahí le sale ese mensajito de comprobación para que ya la persona confirme el voto que está ejerciendo, y una vez que ya le da al cuarto paso el sistema automáticamente le indica que el voto fue elaborado de manera satisfactoria, y ya la persona no podría ejercer un segundo voto en caso de que quisiera intentar nuevamente, entonces básicamente esas pantallitas es el paso a paso……..

Indica el señor Mora Muñoz que: ese cuadrito que está ahí detallado es el resumen de los resultados que se obtuvo de la primera ronda, y tomando en cuenta la cantidad de personas que están inscritas en el padrón electoral, y que es la totalidad de las personas funcionarias activas, teníamos que para que la papeleta quedará electa tenía que alcanzar un total de 196 votos válidamente emitidos, en este caso como vemos ahí la papelea N° 1 únicamente obtuvo 98 votos, se emitieron 26 votos en blanco y 10 votos en nulo para un total de 134, entonces de acuerdo con los artículos que vamos a ver más adelante en esta primer ronda no se alcanzó una papeleta electa……..

Resultados primera ronda:

JUNTA ADMINISTRATIVA DEL SERVICIO ELÉCTRICO MUNICIPAL DE CARTAGO
TRIBUNAL DE ELECCIONES
VOTACIONES DEL J.R.L.
08 DE NOVIEMBRE DEL 2022

CENTRO VOTACION	TOTAL DE VOTANTES	PAPELETA #1	VOTOS EN BLANCO	VOTOS NULOS
EDIFICIO CENTRAL	**31**	20	8	3
EDIFICIO FÁTIMA	**66**	48	13	5
EDIFICIO BARRO MORADO	**1**	1	0	0
EDIFICIO C.C. EL BOSQUE	**10**	9	1	0
EDIFICIO TUIS	**6**	6	0	0
EDIFICIO BIRRIS	**9**	8	1	0
EDIFICIO INFOCOMUNICACIONES	**11**	6	3	2
TOTALES:	**134**	**98**	**26**	**10**

Total del Padrón Electoral	**391**
Votos Emitidos	***134***
Mitad de votos válidos emitidos más 1	***196***
Papeleta Electa	***no hay elección***

Fuente: Tribunal Electoral.

Continua don Arnold Mora indicando que: tomando en cuenta los artículos que están establecidos en las disposiciones generales, fue cuando fue necesario básicamente realizar un segundo proceso para elegir la respectiva papeleta, en este caso ya en la segunda ronda básicamente era la papeleta que tuviera la mayor cantidad de votos válidamente emitidos…….

- Disposiciones para la elección de los (as) representantes de los trabajadores (as) en la Junta Relaciones Laborales:……

- *"**ARTÍCULO 17.** Quedará electa la papeleta que obtenga la mayoría de votos válidamente emitidos, siempre que estos en total representen la mitad más uno de los funcionarios que conforman el padrón electoral……...*
- ***ARTÍCULO 18.** En caso de ser necesaria una segunda elección, el Departamento Talento Humano convocará a elecciones dentro de los cinco días hábiles siguientes a la declaratoria del resultado de la primera elección, utilizando el mismo padrón de esta primera elección."……....*

Interviene don Lizandro Brenes para indicar: don Arnold (Mora), perdón que lo interrumpa, para que conste la entrada don Salvador (Padilla) a las 20:12, y la de don Alexander (Mejías) a las 20:13. Gracias. Procede don Arnold Mora a indicar: aquí está el resultado propiamente de la segunda ronda, vemos que en este caso se obtuvo un total de 187 votos emitidos, la papeleta N° 1 alcanzó un total de 136, se obtuvo 34 votos en blanco, y se emitieron un total de 17 votos nulos. En este caso la papeleta N° 1 con esos resultados quedó electa de acuerdo con lo que se establece en las disposiciones…….

Resultados segunda ronda:

JUNTA ADMINISTRATIVA DEL SERVICIO ELÉCTRICO MUNICIPAL DE CARTAGO
TRIBUNAL DE ELECCIONES
VOTACIONES DEL J.R.L.
16 DE NOVIEMBRE DEL 2022

CENTRO VOTACION	TOTAL DE VOTANTES	PAPELETA #1	VOTOS EN BLANCO	VOTOS NULOS
EDIFICIO CENTRAL	27	19	4	4
EDIFICIO FÁTIMA	101	71	17	13
EDIFICIO BARRO MORADO	4	4	0	0
EDIFICIO C.C. EL BOSQUE	10	8	2	0
EDIFICIO TUIS	10	8	2	0
EDIFICIO BIRRIS	21	16	5	0
EDIFICIO INFOCOMUNICACIONES	14	10	4	0
TOTALES:	**187**	**136**	**34**	**17**

Total del Padrón Electoral	**390**
Votos Emitidos	***187***
Papeleta Electa segunda ronda	***Papeleta #1***

Fuente: Tribunal Electoral.

……..

……..

Continúa el señor Mora Muñoz indicando que: el artículo que N° 19 indica que en una segunda elección quedara electa la papeleta que obtenga la mayoría de votos válidamente emitidos, entonces con base en este artículo fue donde el tribunal declaró electa la papeleta N° 1……..

- Disposiciones para la elección de los (as) representantes de los trabajadores (as) en la Junta Relaciones Laborales:……

  - ***ARTÍCULO 19****. En una segunda elección quedará electa la papeleta que obtenga la mayoría de votos válidamente emitidos. Si en una segunda elección se produce un empate, la suerte decidirá mediante el lanzamiento de una moneda…….....*

Externa don Arnold Mora que: con base en los resultados la recomendación que estamos emitiendo desde Talento Humano es la siguiente:……..

- Juramentar a las funcionarias **Ana Maria Araya Brenes, cédula 03-0402-0994; Deyanira Vigott Castillo, cédula 03-0410-0134; Sonia Espinoza Brenes, cédula 03-0423-0921** en calidad de propietarias y a las señoras **Ana Margarita Cortés González, cédula 03-0379-0763 y Karen Brenes Masis, cédula 03-0378-0693** como suplentes, todas como representantes de los Trabajadores ante la Junta de Relaciones Laborales (JRL), esto de conformidad con los resultados obtenidos luego del proceso de votaciones realizado el pasado miércoles 16 de noviembre del 2022.

Comenta el señor Mora Muñoz que: básicamente ese fue a grandes rasgos el proceso que realizamos con base en las disposiciones, y si lo tienen a bien con el proceso de juramentación, esa sería la presentación……

Resalta don Lizandro Brenes que: como parte la presentación don Francisco (Calvo) se quiere referir también……

Indica don Francisco Calvo: algo muy rápido, adicional a lo que explicaba don Arnold (Mora) que es la el resultado de una elección para los representantes de los trabajadores, igualmente en la Junta de Relaciones Laborales hay representantes de la Administración que son 3, estos no se eligen por elección sino que los elige en este caso la Gerencia General, de esos 3 hay 2 que están vigentes y hay otro que

hay que proponer, entonces en este ahí dentro de la información de la Junta Directiva se les indica que se está proponiendo, o que la Gerencia seleccionó a don Cristian Acuña ahí se explican las razones por las cuales se elige a él, y también ya formando parte del grupo de compañeros que se estarían juramentando dentro de esta sesión……

Interviene don Arnold Mora para indicar que: en el caso de doña Deyanira Vigott se debe hacer la observación que ella por un caso de incapacidad no se encuentra el día de hoy, entonces quedaría para una posterior juramentación……..

Indica don Lizandro Brenes: como es solo una juramentación se le puede hacer el espacio en una próxima sesión; muy bien, en discusión este asunto…….

Desea saber doña Rosario Espinoza: ¿porque creen que haya tan poca participación de los funcionarios?.....

Comenta don Arnold Mora: en los últimos procesos de elecciones hemos tenido ese patrón, a pesar de que de parte nuestra y de la misma Administración se insiste en que los compañeros formen parte de los procesos, ya sea conformando papeletas o ejerciendo el voto, si ha costado un poquito, tal vez es un patrón que se repite ya por otros temas de procesos de elección, pero de parte nuestra hacemos el esfuerzo para que la gente participe, y como les digo que conforme papeletas para que el proceso sea más enriquecedor, pero sí es algo en lo que tenemos que trabajar un poquito más a nivel de comunicación para que en estos procesos exista una mayor participación……...

Externa el señor Calvo Solano que: hay que considerar que está Junta de Relaciones Labores una de las funciones más importantes que hace es recibir un informe de un órgano director, que al final de cuentas está recomendando una sanción a un compañero en la mayoría de los casos, entonces los miembros de ésta Junta tienen que analizar sí recomiendan o no aplicar esa sanción, si llegan o no a las mismas conclusiones que el órgano director, entonces para mucha gente eso puede ser incómodo, porque al final de cuentas por ejemplo; es recomendar sancionar a un compañero, verdad, tampoco es

que sea algo gravísimo pero puede ser una situación en la que mucha gente se sienta incomoda, y que en este caso prefieran no estar en esa situación……

Comenta doña Ana Lía Solano que: en relación a la observación de don Francisco (Calvo), la idea es que se concientice a las personas de que no puede ser, verse como algo problemático, porque al fin y al cabo el que se le haga un procedimiento a un funcionario qué tal vez no está haciendo lo correcto pues, es enriquecedor para no cometer nuevamente el error, y después ¿usted cree que afectó la pandemia? O la virtualidad, ya que es un proceso que se hizo virtual ahora verdad la votación, entonces para ellos era como novedoso, ¿podría creerse eso?.....

Externa el señor Mora Muñoz que: de hecho en el 2020 que fue cuando estrenamos digámoslo así esta aplicación, en ese caso fue para la elección de los representantes de los trabajadores ante la Junta Directiva del FAG, ahí fue cuando estrenamos esta aplicación, más bien consideramos que el proceso se agiliza, porque en cada centro de trabajo los compañeros tienen ahí habilitadas algunas computadoras en donde pueden llegar y ejercer el voto de una manera más fácil en realidad, en el caso de los administrativos igual asumimos que es un proceso más fácil porque cada uno nada más se mete al enlace y ejerce el voto en el momento que lo considere apropiado, no consideramos que haya sido el tema de la virtualidad, sino más bien, es como lo indica muy bien Francisco (Calvo), tal vez es por el tipo de función que van a ejercer en esa Junta, principalmente por el tema de los procedimientos administrativos que genere esa renuencia a participar y a formar parte de la Junta como tal, pero más bien consideramos que el proceso de la virtualidad ha venido a facilitar el proceso de elecciones como tal……..

Externa don Lizandro Brenes: vamos a pasar a la propuesta de acuerdo……..

Resalta doña Anelena Sabater que sería:……..

- Dar por recibido los siguientes documentos: 1. Oficio Nº GG-859-2022 suscrito por el Lic. Francisco Calvo Solano, Gerente General; 2. Oficio Nº SUBG-TH-0798-2022, suscrito por el Lic. Arnold Mora Muñoz, Jefe a.i. Departamento Talento Humano y Licda. Magaly Cáseres Madrigal, Profesional

Nivel 2 Talento Humano; 3. Presentación Elecciones JRL; Oficio Nº GG-858-2022 suscrito por el Lic. Francisco Calvo Solano, Gerente General……...

- Juramentar a las funcionarias Ana Maria Araya Brenes, cédula de identidad 03-0402-0994; Sonia Espinoza Brenes, cédula de identidad 03-0423-0921 en calidad de propietarias y a las señoras Ana Margarita Cortés González, cédula de identidad 03-0379-0763 y Karen Brenes Masis, cédula de identidad 03-0378-0693 como suplentes, todas como representantes de los Trabajadores ante la Junta de Relaciones Laborales (JRL), por el periodo comprendido entre el 24 de noviembre de 2022 al 23 de noviembre de 2025, ambas fechas inclusive……
- Juramentar al funcionario Cristian Acuña Brenes, cédula 03-0353-0057, como representante de la parte patronal ante la Junta de Relaciones Laborales (JRL), por el periodo comprendido entre el 24 de noviembre de 2022 al 23 de noviembre de 2025, ambas fechas inclusive……

Resalta don Lizandro Brenes: entramos a votación, como estamos presenciales, quienes estén a favor de la propuesta de acuerdo por favor sírvanse levantar la mano; queda aprobado, está a favor todo el mundo, ahora vamos a votar a la firmeza, quienes estén a favor de la firmeza; entonces ahora sí, queda aprobado y en firme con 7 votos presentes……

SE ACUERDA: de manera unánime y afirmativa, con siete votos presentes……

4.a. Dar por recibido los siguientes documentos: 1. Oficio Nº GG-859-2022 suscrito por el Lic. Francisco Calvo Solano, Gerente General; 2. Oficio Nº SUBG-TH-0798-2022, suscrito por el Lic. Arnold Mora Muñoz, Jefe a.i. Departamento Talento Humano y Licda. Magaly Cáseres Madrigal, Profesional Nivel 2 Talento Humano; 3. Presentación Elecciones JRL; Oficio Nº GG-858-2022 suscrito por el Lic. Francisco Calvo Solano, Gerente General……

4.b. Juramentar a las funcionarias Ana Maria Araya Brenes, cédula de identidad 03-0402-0994; Sonia Espinoza Brenes, cédula de identidad 03-0423-0921 en calidad de propietarias y a las señoras Ana Margarita Cortés González, cédula de identidad 03-0379-0763 y Karen Brenes Masis, cédula de identidad 03-0378-0693 como suplentes, todas como representantes de los

Trabajadores ante la Junta de Relaciones Laborales (JRL), por el periodo comprendido entre el 24 de noviembre de 2022 al 23 de noviembre de 2025, ambas fechas inclusive……..

4.c. Juramentar al funcionario Cristian Acuña Brenes, cédula de identidad 03-0353-0057, como representante de la parte patronal ante la Junta de Relaciones Laborales (JRL), por el periodo comprendido entre el 24 de noviembre de 2022 al 23 de noviembre de 2025, ambas fechas inclusive……..

Ingresan al recinto los funcionarios a juramentar……...

Procede la Presidencia de Junta Directiva a brindar juramento a los funcionarios representantes de la Junta de Relaciones Laborales……

Se retiran del recinto los señores Ana Maria Araya Brenes, Sonia Espinoza Brenes, Ana Margarita Cortés González, Karen Brenes Masis y Cristian Acuña Brenes, ya debidamente juramentados……..

ARTÍCULO 5.- INFORME SOBRE CIBERATAQUE A LA INFRAESTRUCTURA TECNOLÓGICA DE JASEC ABRIL 2022.

Se conocen los siguientes documentos: 1. Oficio Nº GG-860-2022 Junta Directiva ciberataque, suscrito por el Lic. Francisco Calvo Solano, Gerente General; 2. Informe Ciberataque JASEC 2022; suscrito por Ing. Eddy Martínez Picado, Jefe a.i Departamento Control de Contenidos, Infocomunicaciones; 3. Presentación JD Ciberataque JASEC 2022 2; 4. Oficio Nº SUBG-TIC-100-2022 suscrito Ing. Guillermo Gómez Tenorio, Jefe Área de Tecnologías de Información; 4. Resolución Nº RG-54-2022 Lic. Francisco Calvo Solano, Gerente General; 5. Resolución Nº RG-90-2022 Lic. Francisco Calvo Solano, Gerente General.....

Para este punto se encuentra presente el Ing. Eddy Martínez, Jefe a.i Departamento Control de Contenidos, Infocomunicaciones, quien mediante diapositivas presentará este informe……

Externa don Francisco Calvo que: como ya lo habíamos conversado en algún momento, la idea o el objetivo de la presentación de hoy no necesariamente es abordar todos los aspectos o las aristas del tema, pero por lo menos sí que se pueda hacer una presentación integral de lo que conocemos como el

ciberataque que sufrimos en abril de este año, ¿por qué lo va a presentar Eddy?, porque él ahora lo va a explicar un poco más en detalle, cuando se dio el ciberataque uno de los análisis que se hicieron en un grupo de trabajo que se conformó, es a quién le dábamos la dirección o la responsabilidad general de implementar las medidas y tomar las decisiones necesarias para levantar la infraestructura, en ese momento en realidad la situación fue muy crítica porque no podíamos facturar, no podíamos pagar salarios, no podíamos registrar nada en la contabilidad, etcétera y en realidad era una situación sumamente apremiante, muy riesgosa para la empresa, y la decisión que se tomó fue darle esa responsabilidad no a quienes tenían en principio la función de que eso no ocurriera, entonces en realidad se la dimos a Eddy (Martínez) porque él estuvo durante un tiempo ahí y porque tiene la competencia técnica para llevar adelante esta labor; él estaba en otro puesto en Infocomunicaciones, a través de una resolución se le dio esa labor, se le dio la autoridad para instruirle al equipo de trabajo técnico que tenía a cargo la recuperación, y en realidad él es el que nos va a explicar desde su punto de vista qué fue lo que ocurrió, qué fue lo que se hizo, en qué punto estamos, qué hace falta, entre otros aspectos, esa es la razón por la cual él preparó el informe y también nos va ayudar con la presentación esta noche, básicamente……

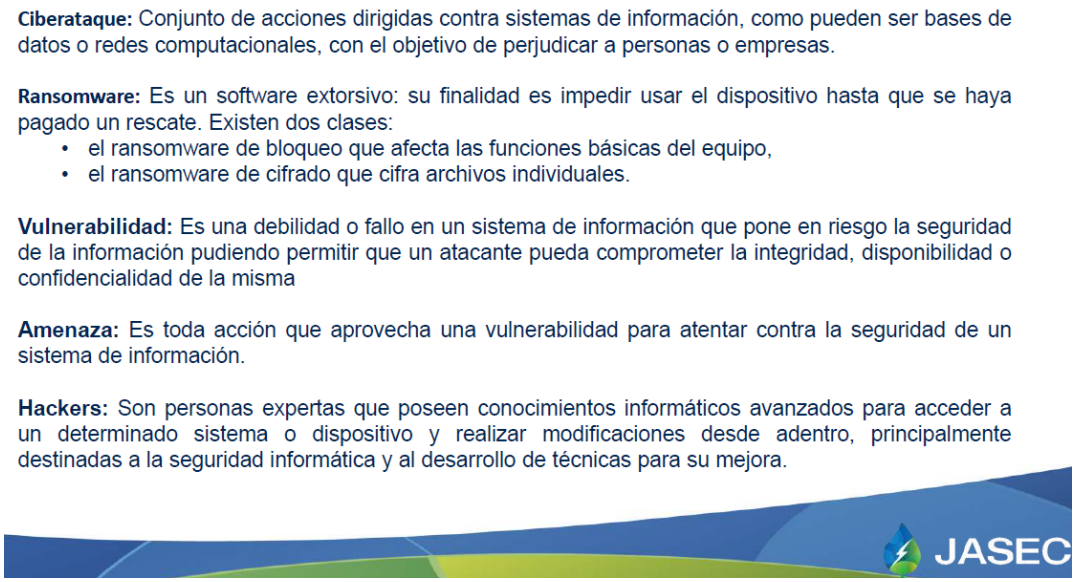
Externa don Lizandro Brenes: muchas gracias don Eddy (Martínez) por estar acá, estábamos hace rato agendando este informe……

Inicia don Eddy Martínez indicando que: sí, como lo indica don Francisco (Calvo) ciertamente mediante una resolución yo le colabore a la gente de TI, en lo que se refiere al restablecimiento de la infraestructura, en ese sentido hace ver que esto del ciberataque digamos que es un poco complejo, y lo primero con lo que voy a iniciar es dando ciertas definiciones como para que ustedes se vayan empapando un poco de qué fue lo que pasó, qué fue lo que se afectó principalmente, la parte de los sistemas, qué fue lo que encontré y que falta por hacer prácticamente…….....

Para los que no conocen qué es un ciberataque, este, es un conjunto de acciones dirigidas contra sistemas de información, como pueden ser bases de datos o redes computacionales, con el objetivo de

perjudicar a personas o empresas, muchas de esas acciones pueden ser a nivel de múltiples operaciones, una de esas es un ransomware, el cual es un virus, pero especializado, cuya finalidad es extorsionar a la víctima pidiendo un rescate, hay 2 tipos de ransomware, el ransomware de bloqueo que afecta las funciones básicas del equipo, y el ransomware de cifrado que cifra archivos individuales, este segundo fue el que tuvo JASEC, a JASEC le entró un ransomware que afectó a la plataforma virtual digamos por decirlo así de servidores y cifró o encriptó los archivos, con cifrar y encriptar me refiero a que los archivos ya no pueden leerse, les cambian la extensión para que me entiendan, no son descifrables, el único que tiene la clave por decirlo así para poderlos descifrar es el atacante, por eso es que ellos solicitan una recompensa, ellos dicen, bueno, si me da tantos millones de dólares yo le comparto la clave, pero eso no siempre es así, a pesar que la víctima pague para tener la clave, no necesariamente te pueden dar la clave, o puede ser que te la den para una cierta cantidad de archivos, o inclusive puede ser que realmente sí te la dan y se mete la clave y des encripta los archivos, pero usted no sabe detrás de eso, sí algo quedó ahí digamos en la infraestructura que muy a futuro pueda volver a ser utilizada para volverte a encriptar, todos esos ransomware se valen de una vulnerabilidad, una vulnerabilidad es un fallo o una debilidad en los sistemas de información, todas estas vulnerabilidades ponen en riesgo los servidores, las aplicaciones, cualquier sistema informático, por eso es muy importante mantener los equipos parchados, equipos me refiero a nivel de sistema operativos, a nivel de hardware digamos el fireware que tienen los equipos, inclusive hasta los mismos sistemas es muy importante tenerlos parchados, justamente porque todos esos parches lo que hacen es corregir una vulnerabilidad existente. Obviamente con las vulnerabilidades existe una amenaza, cuál es la amenaza, es toda acción que aprovecha una vulnerabilidad, entonces posiblemente en la infraestructura hubo alguna vulnerabilidad y la amenaza fue en este caso Conti, que logró descifrar la vulnerabilidad y por ende, pudo entrar; ¿quiénes realizan todo esto del ciberataque? los famosos hackers, que como les mencionaba son personas que poseen muchos conocimientos en informática y son capaces de poder evadir la protección que cualquier empresa pueda llegar a tener, a nivel de hacker existen 3 tipos de

hackers, existen los hackers de sombrero blanco, los de sombrero negro y los de sombrero gris, los hackers de sombrero negro son como Conti los que realmente hacen daño, los hackers de sombrero blanco son los que ellos encuentran una vulnerabilidad pero no la explotan sino que simplemente la encuentran y la dejan ahí, los de sombrero gris son los que a pesar de que la encuentran ellos le avisan digamos a la empresa que tiene una vulnerabilidad para que la corrija…….....



Continúa el señor Martínez Picado indicando que: ya entrando más en contexto de lo que sucedió en JASEC sobre el ciberataque, éste fue ocasionado por Conti, todos vimos en noticias que fue Conti, quién es Conti, el cual es un grupo de personas o hackers como lo dije anteriormente que tienen conocimientos muy avanzados, ellos tienen una organización sumamente organizada, tienen un departamento de Recursos Humanos, tienen un Director, un grupo de desarrolladores, un grupo de hackers, entonces cuando ellos atacan una empresa y logran vulnerar los sistemas de ellos, y al final la empresa logra pagar un rescate, obviamente el rescate se lo dividen entre las personas que estuvieron en el ataque, entonces es toda una organización. ¿Cómo opera?, ellos ingresan a la organización por distintos medios, puede ser mediante un correo electrónico que traía un virus que alguien posiblemente abrió un archivo adjunto, y al abrirlo está listo, o alguien que tal vez entró en internet a una página que no debía entrar y

ya por estar adentro de la organización, para ellos es mucho más fácil ¿por qué?, porque desde adentro de las empresas lo que hacen es que establecen una conexión privada por decirlo así, que no es fácilmente detectable y a través de esa conexión o VPN ellos por ahí es donde se comunican con un servidor central, entonces ellos utilizan el VPN y de ahí se comunican, y si logran descifrar o si logran entrar a las bases de datos por medio de ahí pasan la información y la tienen en un servidor central para el atacado no es fácil darse cuenta. Con respecto al ataque que pasó en Costa Rica, fueron alrededor de 27 personas estatales, dentro de esos está el Ministerio de Hacienda, la Caja (Costarricense del Seguro Social), el Ministerio de Trabajo, nosotros, una universidad de Alajuela, algunas otras empresas privadas que no salieron a la luz, pero más que todo se concentró en las empresas públicas, la estimación que se tiene es que fueron alrededor de $20.0 millones lo que afectó este ataque, y debido a este ataque el Presidente de la República declaró estado de emergencia nacional. En cuanto al impacto en JASEC, este sí fue bastante tal vez ahorita lo vamos a ver más adelante, porque se lograron vulnerar y se lograron encriptar prácticamente toda la infraestructura central, desde los sistemas inclusive hubo un par de máquinas o computadoras de usuario, inclusive un escritorio virtual que había también se logró encriptar, no totalmente pero sí parte de la información. Por otro lado ¿por qué Conti pensó en JASEC?, digamos que no pensó en JASEC, el no dijo uy mirá, JASEC es una empresa de Cartago y pum, sino que ellos simplemente se centraron sobre las empresas Gobierno, comenzaron a hacer test o pruebas para saber dónde era fácilmente entrar y dentro de esos estaba JASEC, entonces por eso fue que lograron ingresar…….

……..

……..

……..

……..

……..

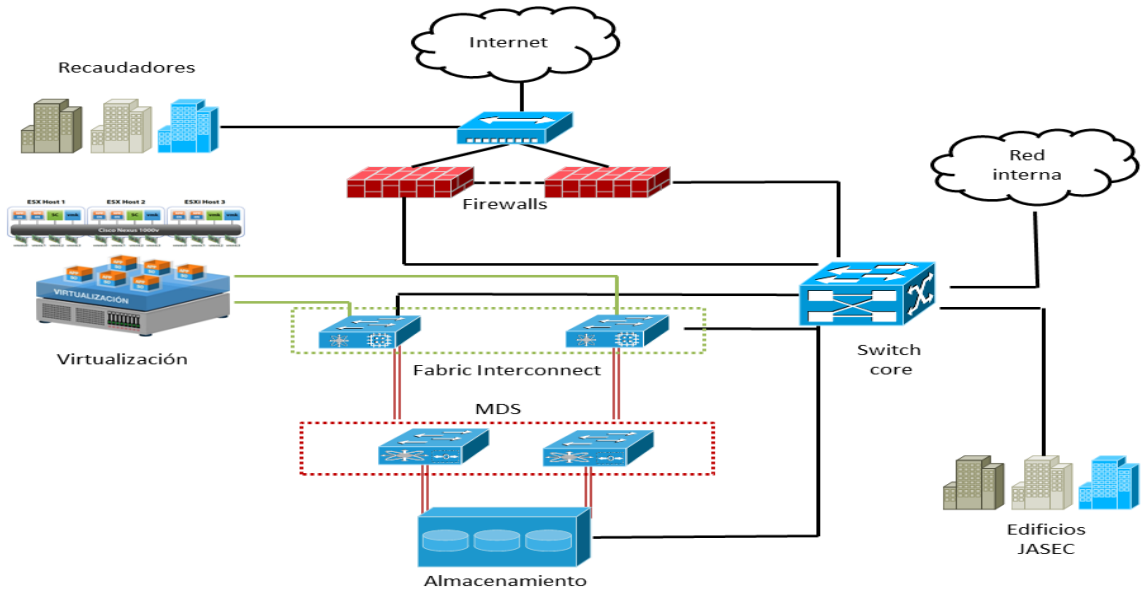
……..

Externa don Eddy Martínez que: sobre el tema de infraestructura informática antes del ataque, la infraestructura que JASEC tiene a nivel de TI está compuesta por múltiples equipos, había un firewall perimetral que es marca Sonicwall, a nivel de comunicación había un Switch central Core, había un Switch Cisco central que es el que administra a nivel de todos los edificios hay un Switch principal por medio de ese Switch principal es por donde pasan obviamente todas las comunicaciones del edificio como tal, y al final ese es el que comunica los demás edificios, después hay otros Switch digamos

equipos de comunicación ya para cada edificio, este edificio tiene sus Switchs de comunicación para interconectar toda la red, Fátima igual y todos los demás edificios. A nivel de este edificio que es donde está el Data Center principal hay una infraestructura de servidores, estos son físicos pero a la vez albergan servidores virtuales adentro, ahorita vamos a ver más adelante, esto también es marca Cisco, también hay un equipo de comunicación de fibra óptica que son los que interconectan los servidores físicos marca Cisco con los almacenamientos que es donde se guardan todos los servidores virtuales y las carpetas compartidas, y obviamente como les indicaba hay unos servidores de almacenamiento, ahí habían 3 servidores de almacenamiento, 2 equipos marca NetApp y 1 Huawei, el Huawei se adquirió a principios de este año……..……..

Comenta el señor Martínez Picado que: la interconexión lógica de todos los equipos que vimos anteriormente se ilustra a continuación: ……

En la parte superior están los dos firewall Sonicwall, a ese firewall Sonicwall se conectaban los distintos recaudadores, se conectaba el internet, posteriormente esos firewall están conectados a Switch por principal, que era el que yo les decía que en cada edificio hay Switch por principal, un equipo de comunicación que es el que permite comunicar los distintos edificios y permite comunicar todas las personas del mismo edificio, a ese Switch principal está interconectado toda la infraestructura virtual que



logran ver ahí, es lo que dice virtualización, Switchs de Fabric que son los Switchs de fibra óptica, los MDS que también fungen en la interconexión, y están los almacenamientos en la parte inferior del diagrama, eso es para que más o menos tenga una idea de cómo entró el virus a JASEC, entró a través de internet, pasó por los firewall, los firewall no lo detectaron, como los firewall no los detectaron llegaron a un Switch por principal, el Switch core principal interconecta toda la infraestructura y todas las máquinas, entonces de ahí paso a la infraestructura virtual, a los almacenamientos y ya estando ahí es simplemente un movimiento lateral, ¿a qué me refiero con movimiento lateral?, el simplemente se mueve de derecha a izquierda……...

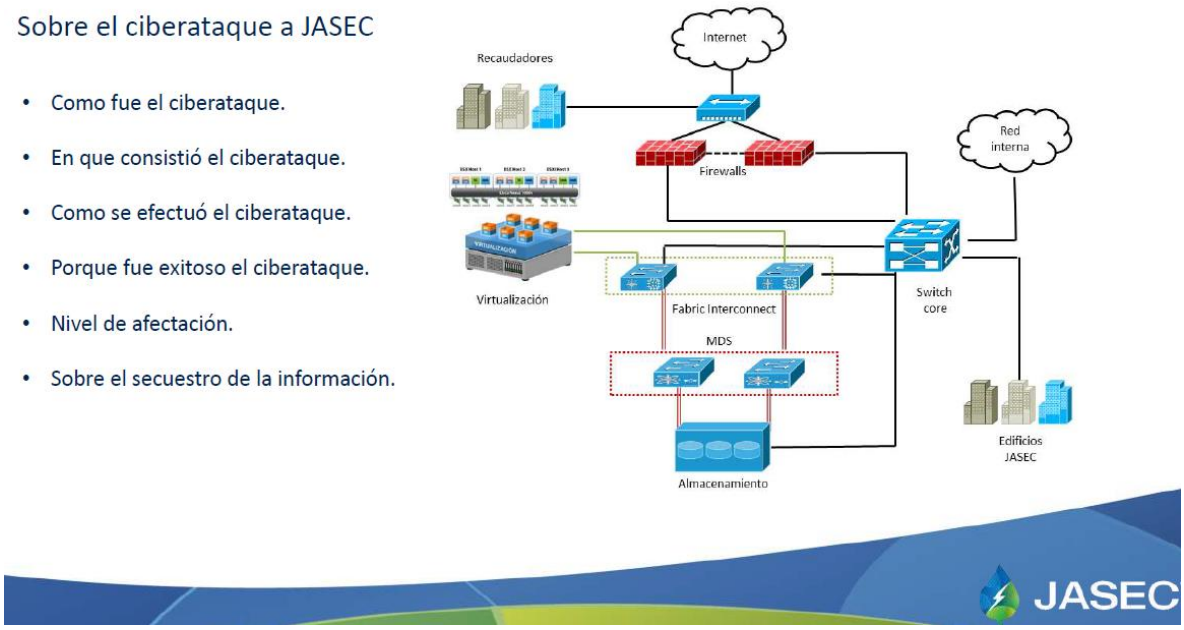
Continúa el señor Martínez Picado indicando que: sobre el ciberataque, ya entrando más en contexto del ciberataque, ¿cómo sucedió el ciberataque?, como yo les indicaba en el siguiente diagrama que en realidad es igual al anterior, el virus o el ransomware entró a través de internet, pasó los firewall y estos no lo pudieron detectar, ésta es la única entrada de JASEC contra el exterior, por eso internet entraba a la página web, al correo electrónico, cuando la gente estaba en teletrabajo por ahí era por donde la gente se conectaba desde las casas de ellos a la infraestructura de JASEC, por medio de un VPN, por medio de un escritorio virtual, por cualquier cosa que la gente intentara conectarse a JASEC desde afuera todo pasaba por ahí, no había otro enlace de internet, JASEC no tenía un segundo enlace de internet, solamente ese. ¿En qué consistió el ciberataque?, consistió en que una vez que ya lograron ingresar a JASEC, a la infraestructura interna, ellos comenzaron a probar hasta donde podían llegar, intentando conectarse a los sistemas, a las bases de datos, a los almacenamientos que fue donde pudieron conectarse y se evidenció el montón de información. ¿Cómo se efectuó? como les indicaba, posiblemente fue por medio de un correo electrónico, de hecho, en las demás instituciones aparentemente fue a través de un correo, alguien abrió un correo, el correo traía algún software malicioso, y ya estando dentro la amenaza ya prácticamente es muy difícil llegar a detectarla, obviamente sí hay herramientas para hacerlo, pero en ese momento JASEC no las tenía. ¿porque fue exitoso el ataque?, fue exitoso primeramente porque los firewalls perimetrales no lo detectaron, y segundo porque

a nivel interno no habían implementadas varias medidas de seguridad, por ejemplo; a nivel de los Switch Core se configuran listas de control de acceso, digamos es una palabra muy informática, son restricciones que uno pone nivel de la red para decir por ejemplo "x" persona solo puede ir a este destino, no puede ir a otra cosa que no esté permitido, y que también principalmente a nivel de antivirus sí estaba configurado, sí estaba funcionando pero habían algunas cosas que tal vez faltaban por hacer por ejemplo; habilitar o bloquear USB´s que es alguna de las cosas que se hizo, con eso se evita que si alguien trae una llave de la casa y la llave viene contaminada no es que la vaya a pegar a la máquina y va a contaminar la máquina, la idea no es esa. En cuanto al nivel de afectación lo vamos a ver ahorita, sí fue, yo lo catalogaría como catastrófico, y sobre el secuestro de la información nunca se logró evidenciar que a nivel de Deep web, y a nivel de la Dark web hubiera información relacionada con JASEC, pero yo la semana pasada o antepasada estuve conversando con un especialista en seguridad que es de Ufinet, ellos son los que nos proveen en Infocomunicaciones el ancho de banda para nosotros poder comercializarlo, y él sí me indicó que vio información de JASEC en la Deep web, dijo que aproximadamente eran 5 gigas de información, él no la compró, porque ustedes saben que a nivel de la Deep web usted tiene que comprar la información, la Deep web es como la parte más oscura del internet, ahí es donde usted compra órganos, armas, él me dijo que inclusive vio información del (Ministerio de) Hacienda, la información del (Ministerio) de Hacienda la vendían en $50.000 aproximadamente y creo que era como 10 gigas de información, y aparentemente era 1 Tera lo que había en la Deep web del (Ministerio de) Hacienda, pero él sí me dijo que en algún momento logró ver información de JASEC, yo le dije que si no la había encontrado otra vez, y lo que me dijo era que iba a buscar otra vez a ver si la encontraba, pero hasta el momento no me ha dicho nada, no sé qué tipo de información será, pero como les digo él si me dijo que la logró ver……..

……..

……..

……..



Externa el señor Martínez Picado que: sobre cómo se efectuó el ataque, en realidad Conti una vez que ingreso lo hizo a través de un origen, ese origen que ven ahí es el servidor que administraba los servidores virtuales, ese que dice 10.6.1.225, una dirección IP es como un identificador por decirlo así que tiene cada equipo que se conecta a la red, entonces digamos todas las computadoras tienen un IP, un Switch tiene una dirección IP, un teléfono tiene una dirección IP, un almacenamiento tiene una dirección IP, todo tiene una dirección IP, entonces una vez que el ransomware entró en esa 10.1.6.225 de ahí se trató de comunicar con la 10.1.5.240 que eso era un almacenamiento, una vez estando ahí comenzó a cifrar información, en esos almacenamientos era donde se guardaban los escritos virtuales, las carpetas compartidas y algunos servidores virtuales, y como ven más abajo ya comenzó a encriptar, ven por ejemplo los archivos que dicen .tEz9Q son los archivos encriptados, ya eso nadie lo puede leer, no hay sistema que lo lea, no hay programa que lo lea porque ya está encriptado……...

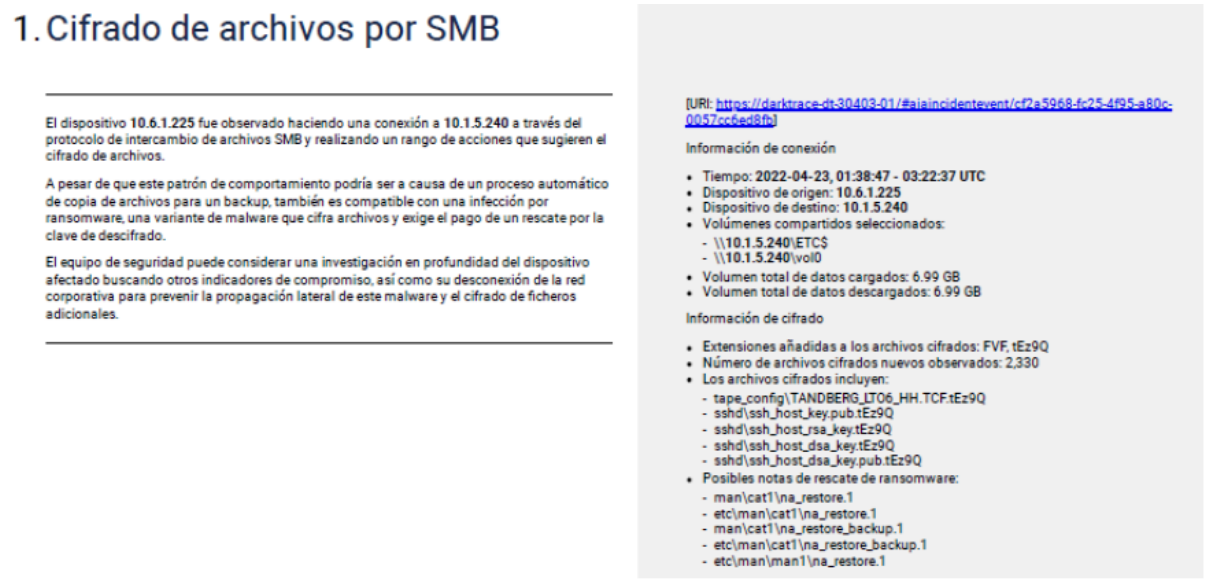
……..

……..

……..

……..

Cómo se efectuó el ataque:



1. Cifrado de archivos por SMB

El dispositivo **10.6.1.225** fue observado haciendo una conexión a **10.1.5.240** a través del protocolo de intercambio de archivos SMB y realizando un rango de acciones que sugieren el cifrado de archivos.

A pesar de que este patrón de comportamiento podría ser a causa de un proceso automático de copia de archivos para un backup, también es compatible con una infección por ransomware, una variante de malware que cifra archivos y exige el pago de un rescate por la clave de descifrado.

El equipo de seguridad puede considerar una investigación en profundidad del dispositivo afectado buscando otros indicadores de compromiso, así como su desconexión de la red corporativa para prevenir la propagación lateral de este malware y el cifrado de ficheros adicionales.

[URI: https://darktrace-dt-30403-01/#aiaincidentevent/cf2a5968-fc25-4f95-a80c-0057cc6ed8fb]

Información de conexión

- Tiempo: **2022-04-23, 01:38:47 - 03:22:37 UTC**
- Dispositivo de origen: **10.6.1.225**
- Dispositivo de destino: **10.1.5.240**
- Volúmenes compartidos seleccionados:
  - **10.1.5.240**\ETC$
  - **10.1.5.240**\vol0
- Volumen total de datos cargados: 6.99 GB
- Volumen total de datos descargados: 6.99 GB

Información de cifrado

- Extensiones añadidas a los archivos cifrados: FVF, tEz9Q
- Número de archivos cifrados nuevos observados: 2,330
- Los archivos cifrados incluyen:
  - tape_config\TANDBERG_LTO6_HH.TCF.tEz9Q
  - sshd\ssh_host_key.pub.tEz9Q
  - sshd\ssh_host_rsa_key.tEz9Q
  - sshd\ssh_host_dsa_key.tEz9Q
  - sshd\ssh_host_dsa_key.pub.tEz9Q
- Posibles notas de rescate de ransomware:
  - man\cat1\na_restore.1
  - etc\man\cat1\na_restore.1
  - man\cat1\na_restore_backup.1
  - etc\man\cat1\na_restore_backup.1
  - etc\man\man1\na_restore.1

Comenta que a continuación también se muestra otra comunicación que realizó el mismo ransomware, pero como ven es otro origen, ya no es el anterior, porque el anterior es 10.1.6.225 ese es 10.1.5.241, eso era un servidor que se tenía para respaldos de información de los usuarios, toda esa información de los usuarios iba desde las máquinas de los usuarios a los almacenamientos, entonces ya podrán imaginarse que fue lo primero que se cifró, los almacenamientos 10.1.5.241 es igualmente un almacenamiento, y como podrán ver ahí hay 3 carpetas compartidas, uno que dice bkp_yahaira y bkp_sipac, esas dos carpetas fueron encriptadas, y de hecho más abajo ven que dice estados de cuenta, diciembre 2020, son archivos de Excel y vean que ya tienen la extensión tEz9Q, esos son ya archivos encriptados……..

……..

……..

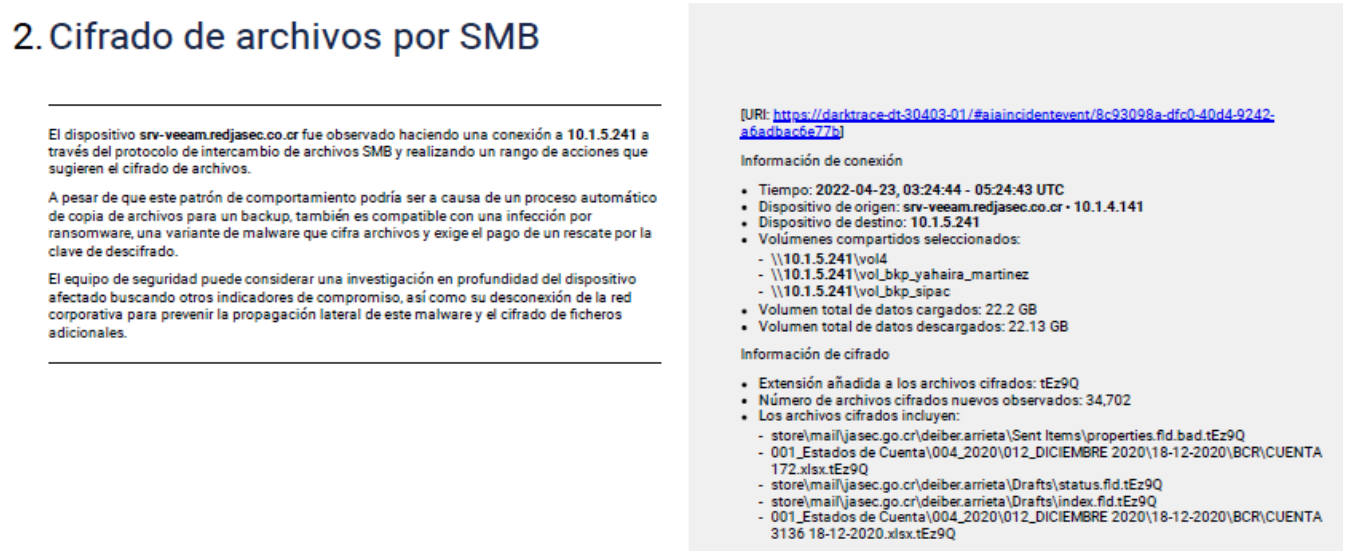
……..

……..

……..

……..

Cómo se efectuó el ataque:



2. Cifrado de archivos por SMB

El dispositivo **srv-veeam.redjasec.co.cr** fue observado haciendo una conexión a **10.1.5.241** a través del protocolo de intercambio de archivos SMB y realizando un rango de acciones que sugieren el cifrado de archivos.

A pesar de que este patrón de comportamiento podría ser a causa de un proceso automático de copia de archivos para un backup, también es compatible con una infección por ransomware, una variante de malware que cifra archivos y exige el pago de un rescate por la clave de descifrado.

El equipo de seguridad puede considerar una investigación en profundidad del dispositivo afectado buscando otros indicadores de compromiso, así como su desconexión de la red corporativa para prevenir la propagación lateral de este malware y el cifrado de ficheros adicionales.

[URI: https://darktrace-dt-30403-01/#aiaincidentevent/8c93098a-dfc0-40d4-9242-a6adbac6e77b]

Información de conexión

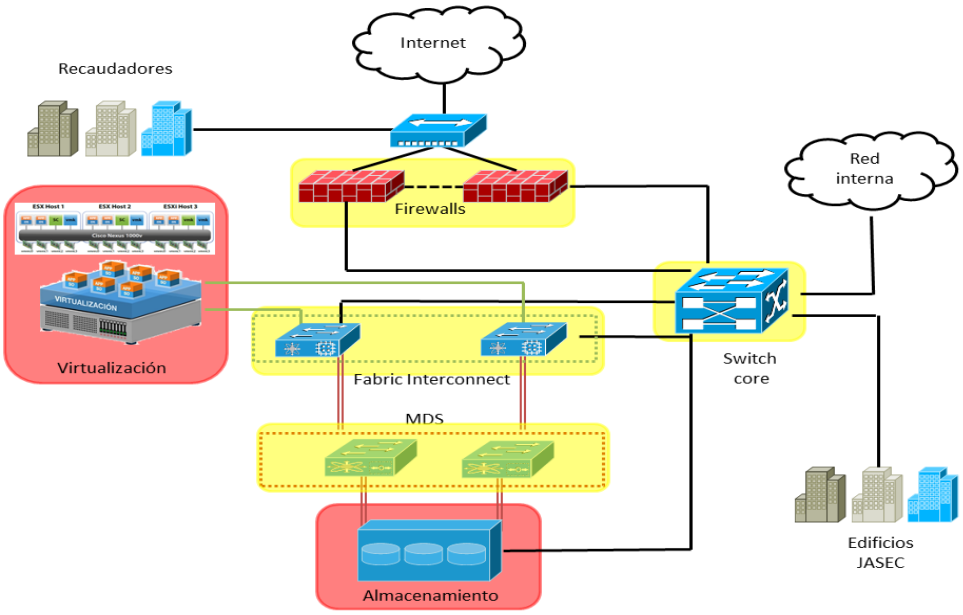
- Tiempo: **2022-04-23, 03:24:44 - 05:24:43 UTC**
- Dispositivo de origen: **srv-veeam.redjasec.co.cr - 10.1.4.141**
- Dispositivo de destino: **10.1.5.241**
- Volúmenes compartidos seleccionados:
  - **10.1.5.241**\vol4
  - **10.1.5.241**\vol_bkp_yahaira_martinez
  - **10.1.5.241**\vol_bkp_sipac
- Volumen total de datos cargados: 22.2 GB
- Volumen total de datos descargados: 22.13 GB

Información de cifrado

- Extensión añadida a los archivos cifrados: tEz9Q
- Número de archivos cifrados nuevos observados: 34,702
- Los archivos cifrados incluyen:
  - store\mail\jasec.go.cr\deiber.arrieta\Sent Items\properties.fld.bad.tEz9Q
  - 001_Estados de Cuenta\004_2020\012_DICIEMBRE 2020\18-12-2020\BCR\CUENTA 172.xlsx.tEz9Q
  - store\mail\jasec.go.cr\deiber.arrieta\Drafts\status.fld.tEz9Q
  - store\mail\jasec.go.cr\deiber.arrieta\Drafts\index.fld.tEz9Q
  - 001_Estados de Cuenta\004_2020\012_DICIEMBRE 2020\18-12-2020\BCR\CUENTA 3136 18-12-2020.xlsx.tEz9Q

Continúa don Eddy Martínez indicando que: sobre ¿cuál fue el nivel de afectación?, este es el que se visualiza en el cuadrito rojo, que son los almacenamientos que era donde se guardaba absolutamente toda la información que tenía JASEC, servidores virtuales, aplicaciones, correo electrónico, página web, carpetas compartidas, todo absolutamente todo con lo que JASEC trabaja estaba ahí, y por ende también la solución de virtualización, la solución de virtualización está compuesta por 4 servidores físicos, un servidor físico para virtualización es un servidor muy robusto que tiene mucha memoria RAM y mucho procesador, ¿por qué?, porque en el momento que el administra los servidores virtuales el provee recursos a los servidores virtuales para que esos puedan funcionar, entonces por ejemplo, los servidores virtuales que tiene JASEC físicos tienen 196 gigas de RAM, eso abarca 4 servidores, y 196 por 4 equivale a casi 800 gigas de memoria RAM, esos 800 gigas al final los equipos físicos se las brindan a los servidores virtuales, para que los servidores virtuales puedan ser aprovisionados y puedan funcionar. También obviamente tienen procesador, el procesador funciona igual, y el almacenamiento, ya esos servidores digamos no tienen tanto disco duro, el almacenamiento se lo proveen los equipos de almacenamiento, ellos simplemente les proveen a los servidores virtuales memoria RAM y procesador, el almacenamiento se lo da los propios servidores de almacenamiento, que son los 3 que mencionaba yo anteriormente, los 2 NetApp y el Huawei, entonces lo que está enmarcado en rojo es lo que se afectó

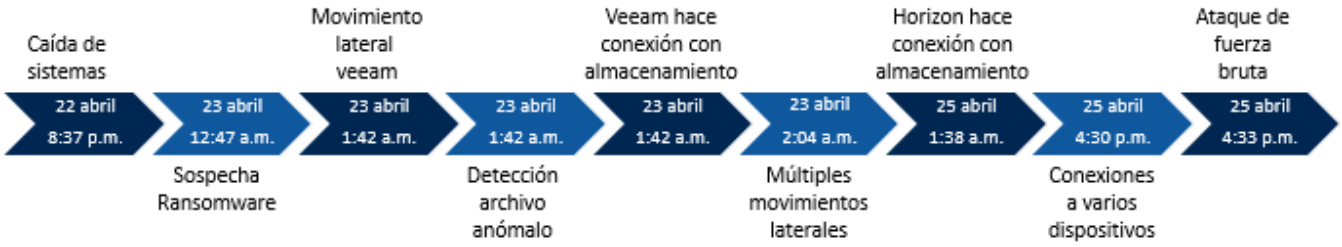
directamente, lo que está en amarillo es por donde el virus pasó y no fue detectado, osea digamos que entre comillas fue vulnerado, aunque nunca se llegó a comprobar que realmente, salvo los fireware nunca se logró comprobar que hubiera algo ahí…….



Resalta el señor Martínez Picado que: a continuación se muestra una línea de tiempo, desde que pasó el ataque el día 22 de abril a las 8:37 más o menos, yo ya no estaba en TI, yo estaba en Infocomunicaciones, pero yo sí me di cuenta ya que tenía mucha conversación con los compañeros de soporte, y justamente en ese momento la gente de Infocomunicaciones nos reportó que no tenían acceso a los sistemas, que algo pasó, entonces yo comencé a preguntarles y ya ahí empezamos a conversar, que se había caído que no podían reestablecerlo y otro montón de conversación que teníamos ahí, ya el 23 de abril a las 12:49 ya hubo una sospecha de ransomware, el 23 de abril a la 1:42 hubo un movimiento lateral, esto es lo que digo sobre que una vez que el virus ya llega a un punto él no se mueve de arriba para abajo, no es que el pasa de los servidores a los equipos de usuario, sino que él se mueve solamente de derecha a izquierda, si él está en la infraestructura de servidores el solamente se mueve ahí, y eso fue justamente lo que hizo, se movió a nivel de todos los servidores virtuales y de toda la infraestructura que estaba ahí, y ahí se quedó hasta que nos logró encriptar, y hasta que fue descubierto, el mismo 23 a la 1:42 se detectó un archivo anómalo, digamos un archivo extraño, igualmente a la 1:42

el Veeam que es un equipo que es donde yo les indicaba que se guardaban los respaldos, él hace una conexión al almacenamiento y comienza a encriptar datos, él hace igual múltiples movimientos laterales, el Horizon que ese es el otro servidor que yo les indicaba que es 10.1.6.225 que era el que administraba los escritorios virtuales, también hizo un intento de conexión hacia los almacenamientos, luego hay varias conexiones, esto ya fue el día lunes 25, ese mismo día ya hay varias conexiones, y el mismo lunes se produce o se detecta un ataque de fuerza bruta, éste es cuando alguien no sabe la clave o los credenciales para entrar entonces él lo obliga a entrar, trata, trata y trata de entrar, eso es un ataque de fuerza bruta, hasta que llega un punto en que logra entrar……...

Línea de tiempo del ciberataque:



Continúa el señor Martínez Picado indicando: ¿cuáles fueron los hallazgos encontrados al inicio de la recuperación?, cuando ya la Gerencia me designa a mí para venir a ayudarle a TI se hace una revisión física de los equipos, obviamente yo tenía que darme cuenta cuál fue el nivel de afectación, cómo estaban los equipos a nivel físico, se hicieron pruebas obviamente controladas de conexión a los equipos vulnerados ahí igualmente solamente se utilizó una computadora, esa computadora sólo se utilizó para conectarse a los equipos que estaban vulnerados nada más, no podía conectarse a otro lado, porque no sabíamos si al momento que yo conectaba la computadora los equipos vulnerados la maquina se iba a contaminar, entonces yo no podía después llevarme esa máquina para conectarla a la red, sino iba a ser un desastre, también se revisaron con las configuraciones de los equipos, con esto me refiero a los Switchs, los firewalls, a la solución de virtualización, y obviamente también se extrajo esa configuración para número 1 poder revisarla, número 2 para tenerla como respaldo o como evidencia, y número 3

porque en el momento que los equipos tenían que ser reinstalados digamos, si por “x” o “y” razón alguno llegaba a funcionar se tenía respaldo, entonces más o menos se podía ver como estaba antes de……..

Hallazgos

- Revisión física de los equipos……..
- Pruebas controladas de conexión a los equipos vulnerados……..
- Accesos controlados a las configuraciones de los equipos……..
- Extracción de configuración si ser alterada……

Externa don Eddy Martínez que: las siguientes imágenes muestran más o menos los archivos que se lograron encontrar que estaban encriptados, los 2 corresponden a los almacenamientos, como ven ahí hay archivos punto Conti, en la imagen de la izquierda se muestran los archivos de los servidores virtuales, y la imagen de la derecha esos si son archivos propios del almacenamiento, aquí no se encriptaron solamente los servidores, sino que también se encriptó los sistemas operativos de los equipos como tal, digamos los almacenamientos igualmente tienen un sistema operativo, los servidores para virtualización tienen un sistema operativo, todo eso se encriptó, no es solamente la información de JASEC sino los equipos como tal digamos, no hablando de equipos de comunicación Switchs y router, pero sí los servidores y los almacenamientos, todo se encripto, entonces más adelante lo vamos a ver, pero para restablecimiento obviamente tuvo que reinstalarse todo……

……..

……..

……..

……..

……..

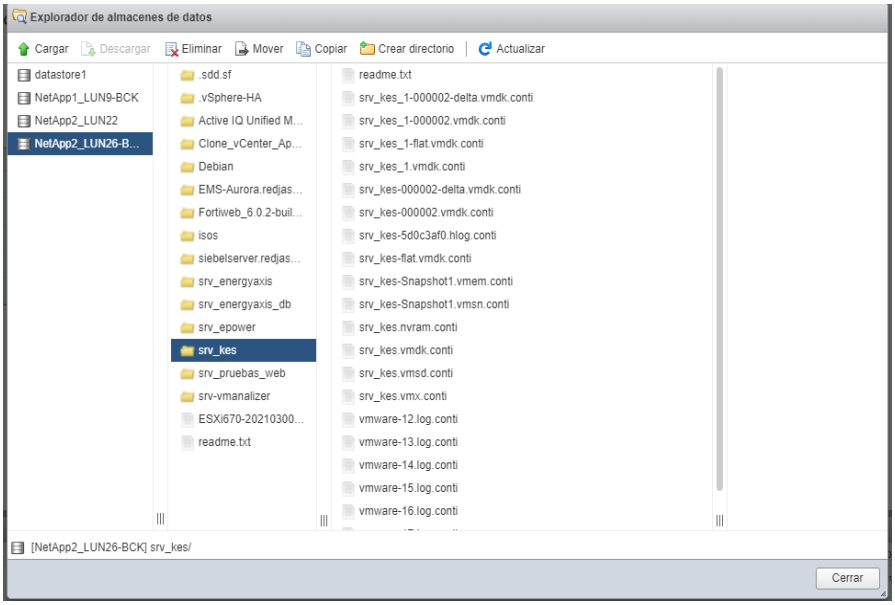
……..

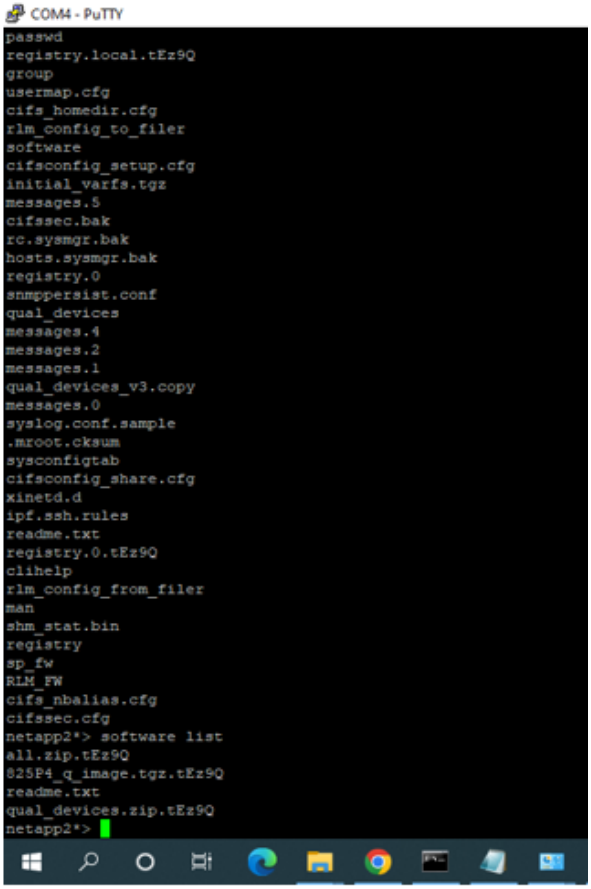
……..

……..

Hallazgos

Encriptación de los archivos

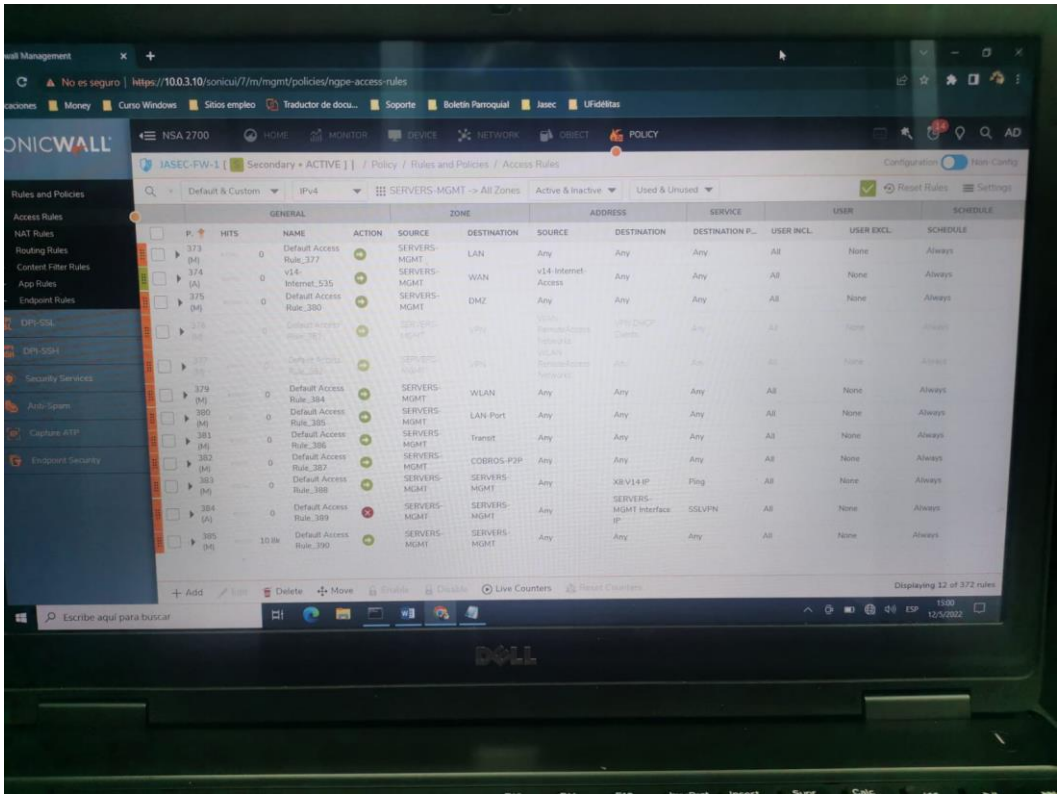




Indica el señor Martínez Picado que: a nivel de firewall se logró encontrar que habían políticas que no estaban bien configuradas, digamos cuando uno configura un firewall, un origen y un destino tiene permiso para conectarse a tal cosa, entonces digamos que tiene que haber una política que diga, los usuarios del edificio central, o los usuarios de plataforma, facturación van a salir a internet a este destino, y sólo exclusivamente a estos puertos, a los puertos, me refiero solamente a enviar correos, solamente a conectarse a “x” o “y” página, y en la configuración como pueden ver ahí está abierto para todo, ahí prácticamente está conéctese a todo, y eso a nivel de buenas prácticas de seguridad no debe ser así, ahí se puede visualizar que hay una parte de servidores, como ven hay un origen dice en y destino a lo que sea dónde dice “Any” que es cualquier origen, destino “Any” a lo que sea, y donde dice service que

es el puerto por decirlo así vean que dice “Any” entonces cualquier cosa de origen, cualquier cosa destino, puede conectarse a cualquier cosa……...

Políticas de seguridad en el firewall



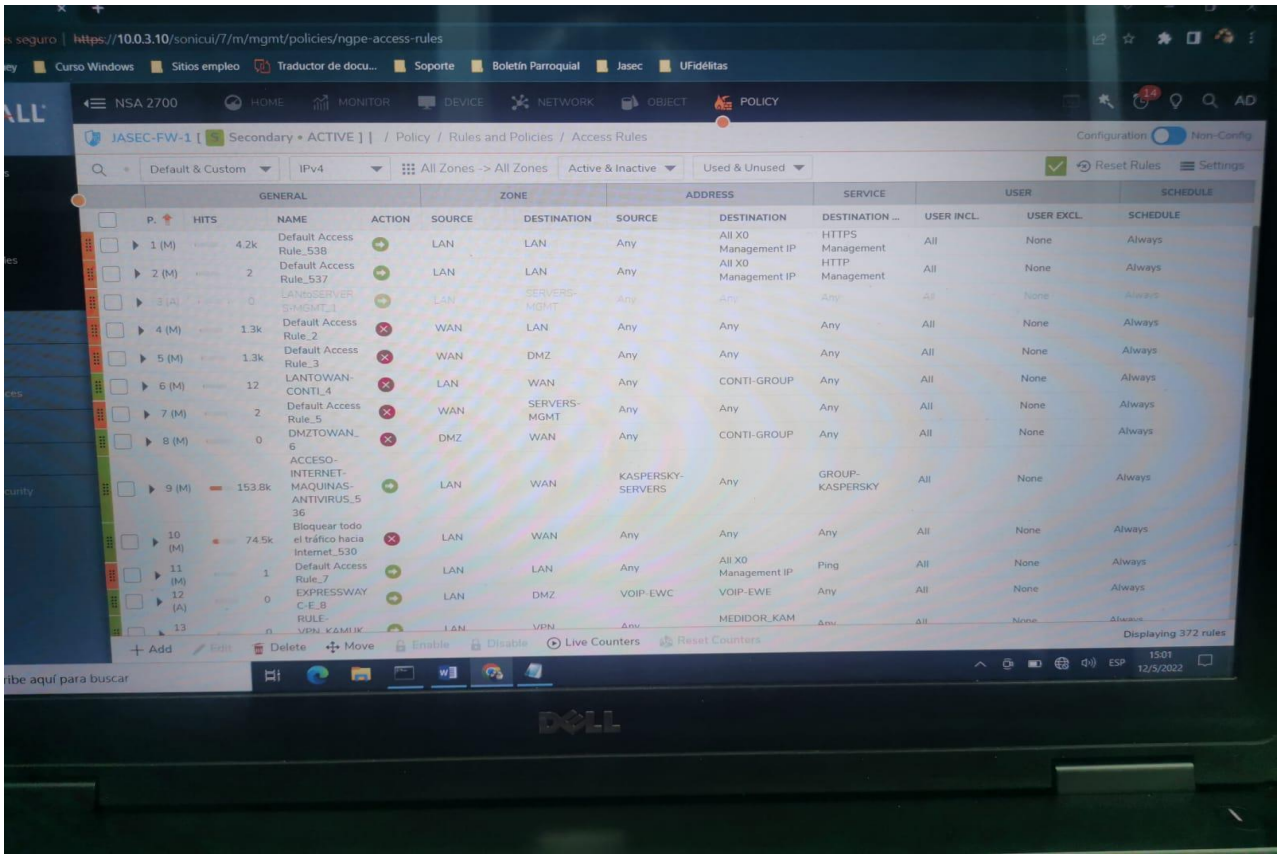
Externa que a continuación se ilustra otra captura que se hizo, esas políticas son las de firewall perimetral que en ese momento estaban configuradas, ahí obviamente hay algunos que estaban bloqueadas, posiblemente la gente de TI cuando se detectó el ataque ven uno que dice Conti Group, y posiblemente fueron las direcciones IP que en ese momento el Gobierno anunció que eran las de Conti, ellos las bloquearon pero ya ahí no había mucho que hacer, eso es para que tal vez las máquinas internas no se continuaran comunicando con Conti……

……..

……..

……..

Políticas de seguridad en el firewall



Indica don Eddy Martínez que: a nivel de tecnología muchas veces nosotros nos apoyamos obviamente en estudios digamos que hagan las diferentes empresas sobre distintas soluciones, una de esas empresas es Gartner está es una empresa que hace o evalúa distintas soluciones de diferentes tipos, y a uno le da más o menos una idea o lo orienta sobre qué es lo que más aconseja comprar en el mercado, digamos si yo ando buscando no sé un almacenamiento por poner un ejemplo; comienzo a buscar en internet, si Gartner ya hizo una comparación a nivel de todas las marcas de almacenamientos y dice mira sí de las 15 marcas de almacenamiento las que ahorita van de punta y que son las mejores son X, Y, y Z, y yo digo sí voy a comprar esas X, Y, y Z, si hay una marca V por ejemplo, y no está muy bien catalogada no veo porque tengo que comprarla. Ese cuadro que se muestra en la diapositiva es justamente a nivel de firewall, entonces ven a Sonicwall a pesar que está tomado en cuenta en el cuadrante de Gartner se puede observar que es una de las tantas marcas existentes pero no es la mejor,

ven que las líderes son las 3 que están arriba, Palo Alto (Networks), Fortinet y Check Point (Software Technologies), ¿qué pasa?, JASEC antes de comprar los Sonicwall tenía Fortinet, ahorita tenemos un Palo Alto (Networks), y también está ahí, entonces siempre se ha tratado de adquirir equipo que sea líder, confiable, pero en este caso los Sonicwall pues no están dentro del cuadrante de líder……

Cuadrante de Gartner

Proporciona un marco comparativo que facilita la toma de decisiones a la hora de estudiar y contratar el servicio tecnológico más adaptado a las necesidades…….

Source: Gartner (November 2021)

Continúa el señor Martínez Picado indicando que: algunos otros hallazgos que se encontraron, a nivel del almacenamiento Huawei que se compró en marzo no se le había configurado los respaldos, cuando TI compró el almacenamiento lo hizo porque uno de los dos almacenamientos NetApp ya estaba fuera de soporte, ya el fabricante no le daba soporte, osea ya ahí no había nada que hacer, si algo le sucedía al Hardware no había quien le diera soporte, ahí habría que contratar a alguien para que venga a revisar o no sé, entonces TI compró el Huawei, cuando se hizo esa compra ellos los que hicieron fue que movieron los servidores del almacenamiento que ya estaba fuera de soporte y lo pasaron al Huawei, entonces digamos que todo estaba del lado Huawei, pero qué hicieron no le configuraron los respaldos

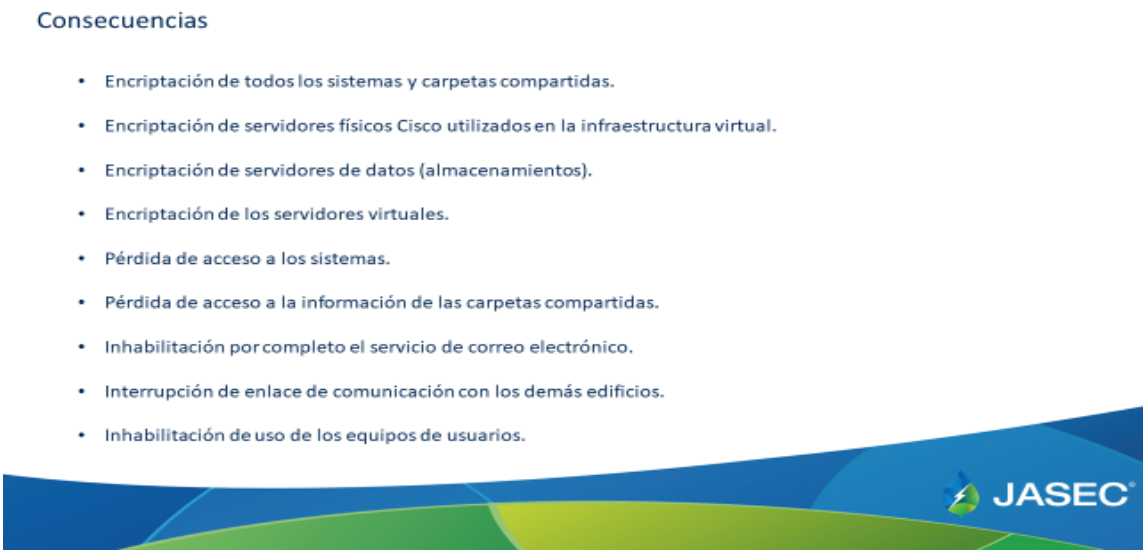
a las máquinas virtuales, entonces sin respaldos y encriptados no hay como recuperarse, no hay, era imposible no había por donde, no había respaldo de nada porque la empresa que hizo la implementación no lo configuró, no estaba configurado. Otro hallazgo que se encontró fue que digamos toda esta infraestructura de virtualización, los servidores, el almacenamiento, no se la había hecho la renovación del soporte, con el soporte me refiero a que si usted por X o Y razón tiene un problema con la infraestructura usted llama al fabricante, y usted indica lo que le está pasando y si hay soporte ellos le ayudan, pero no había, anteriormente había un analizador de vulnerabilidades que era el Nessus, TI no lo había renovado, ya eso no existía, no se compró, por qué no sé, ese analizador vulnerabilidades lo que permite es escanear la red en busca de posibles vulnerabilidades y corregirlas, entonces si se escaneaba el servidor y este tenía X vulnerabilidad usted podía renovar esa vulnerabilidad para que al final no fuera una amenaza dentro de la red, y así no nos pudieran hackear, había un Web Application Firewall que ese es un Firewall o una protección especializada para sitios web, portales, cualquier plataforma web que sea accesible desde afuera, entonces en esto está la página web, el correo electrónico, el portal para conectarse a la solución de virtualización, todo eso estaba protegido por ese Web Application Firewall y este ya no estaba funcionando lo habían quitado no sé porque, como les no estaba lo de renovación de soporte de Cisco, y no se había comprado la renovación del otro NetApp que era donde estaban las carpetas compartidas, gracias a Dios, de ahí sí había respaldo, entonces eso estaba tal cual, como yo lo dejé, entonces gracias a eso pudimos recuperar la información de los usuarios que estaba ahí……

Hallazgos

- Configuración del almacenamiento Huawei……..
- Continuidad de soluciones y soporte de infraestructura…….
    - No se efectuó la renovación del Analizador de vulnerabilidades……..
    - No se continúo utilizando el Web Application Firewall……
    - No se efectuó la renovación del soporte de Cisco UCS……..

- No se efectuó la renovación del soporte del NetApp FAS 2620……..

Comenta don Eddy Martínez: ¿cuáles fueron las consecuencias que tuvo este ciberataque?, mismas que se detallan en la siguiente diapositiva, evidentemente la encriptación de todos los sistemas y carpetas compartidas, encriptación de los servidores físicos, toda la infraestructura virtual está encriptada, la encriptación de los servidores de almacenamiento, eso era donde se guardaban los servidores virtuales, las carpetas compartidas todo se guardaba ahí, la encriptación de los servidores, gracias a toda esa encriptación se perdió el acceso a los sistemas, osea nadie podía entrar a los sistemas institucionales, se perdió la información de las carpetas compartidas, toda la información que los usuarios tenían ahí quedó inaccesible nadie podía consultar la información, se inhabilitó por completo el correo electrónico porque éste estaba en la solución de virtualización, cuando sucedió esto, se le solicitó a TI que interrumpiera la conexión con todos los edificios, aislar a este edificio y por ende, no había comunicación con nadie, y se le pidió a los usuarios no utilizar los equipos, los equipos se desconectaron de la red y nadie podía hacer nada……

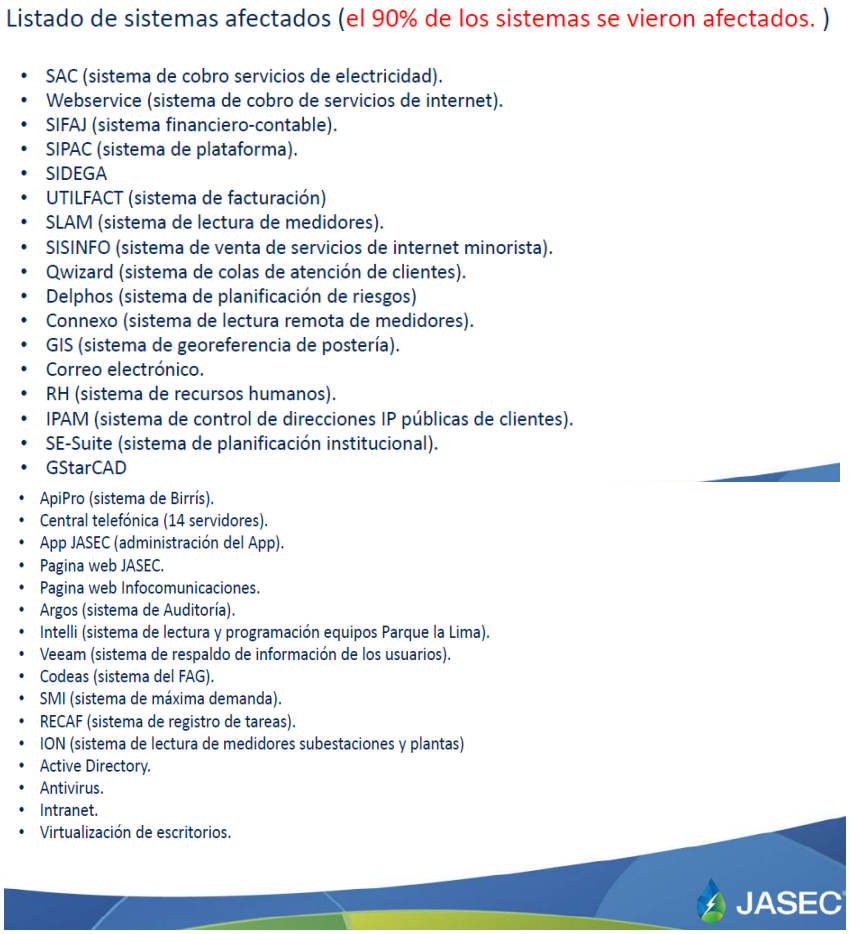


……

……..

……..

En cuanto a los sistemas que se vieron afectados están:……



Resalta el señor Martínez Picado que: es importante aclarar que todo el ataque se concentró solo en éste edificio, lo de SCADA que está en el Bosque, lo de Infocomunicaciones que está en Cerrillos, de eso no se logró vulnerar nada, no se encontró, entonces, eso sí siguió operando, pero lo que estaba en este edificio propiamente ahí sí hubo una encriptación……

Interrumpe don Francisco Calvo para indicar que: desea ampliar un poco lo que está diciendo Eddy (Martínez), si nosotros consideráramos toda la infraestructura tecnológica de JASEC la podemos dividir en 3 grupos: todo lo que está allá en el edificio que ustedes conocieron de Infocomunicaciones ese es un grupo, esa no se vio afectada, hay otro grupo de tecnología o estructura que es la que administra por ejemplo; las redes eléctricas, los patios de interruptores, por ejemplo; lo que ustedes vieron en el Bosque, la que administra las plantas hidroeléctricas, eso normalmente se administra a través de scadas eso no

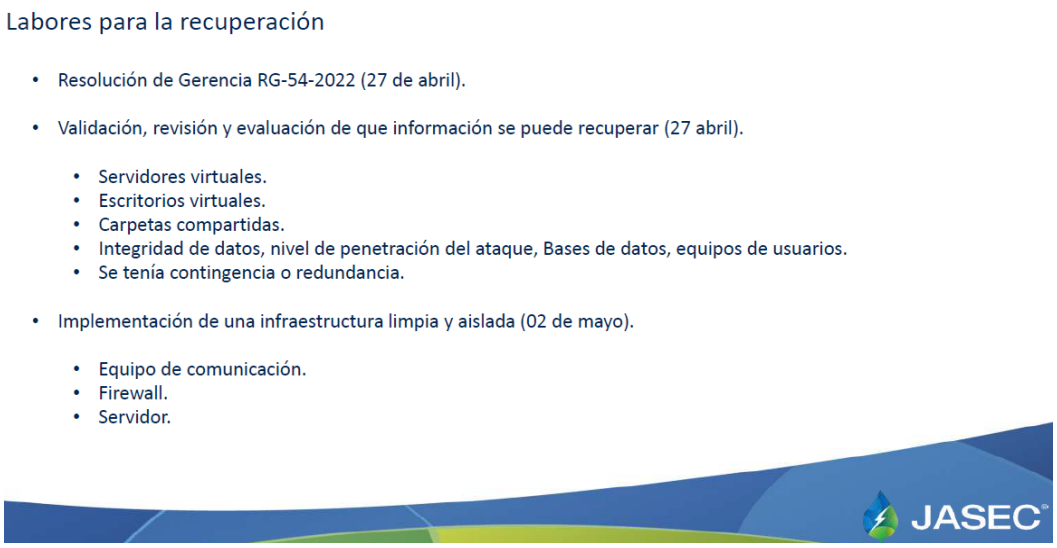
fue afectado, eso es importante porque si al final por ejemplo; se hubiera podido vulnerar esos sistemas por ejemplo; hasta pudieron haber desconectado las redes, parado las plantas, o haber hecho que funcionaran mal, de igual manera en el caso de Infocomunicaciones habría interrumpido el servicio que se da en Infocomunicaciones, esas dos grandes secciones de estructuras no fueron afectadas, pero hay una muy grande que es ésta que está explicando Eddy (Martínez), y yo la llamo como la estructura Comercial, Administrativa y Financiera que es la que está en el Data Center, en este edificio y que digamos que permite que las funciones, o esa infraestructura que permite funciones como recaudar, leer, facturar, hacer los estados financieros, todo el presupuesto, pagar las planillas, y otro montón de sistemas que son los que están acá, entonces esa fue la parte que sí fue afectada, porque es la que está administrada desde éste data center, y aquí fue donde surgió la vulneración que se dio……

Comenta don Eddy Martínez que: ahí obviamente hay sistemas de todo, como lo indica don Francisco (Calvo) desde financiero-contable, Recursos Humanos, Facturación, recaudación, lectura, DELPHOS, lectura remota, de Auditoría, el SE-Suite, correo electrónico, pagina web, Fondo de Ahorro y Garantía, prácticamente todos los sistemas que estaban contenidos en la infraestructura virtual, todos fueron vulnerados y encriptados……...

Ahora bien, una vez que ya se encontraron los hallazgos y se vio el panorama de qué fue lo que pasó, vino todo lo que es el proceso de recuperación, mediante la resolución RG-54-2022 la Gerencia me designa a mí como persona encargada de todo el proceso de recuperación, una vez ya con la resolución se válida, se revisa y se evalúa qué información se puede recuperar, evidentemente no se pudo recuperar nada a excepción de las carpetas compartidas, entonces ahí se revisan los servidores virtuales, se revisó la infraestructura de los escritorios virtuales, las carpetas compartidas, se revisó la integridad de los datos, realmente si los datos estaban íntegros, esto, principalmente de las bases de datos, ¿por qué?, porque en las bases de datos es donde está toda la información digamos de los clientes, ahí es donde se conectan todos los sistemas a los 4-5 servidores de las bases de datos, nosotros no sabíamos a ciencia cierta cómo estaban esos servidores, hay una empresa que está

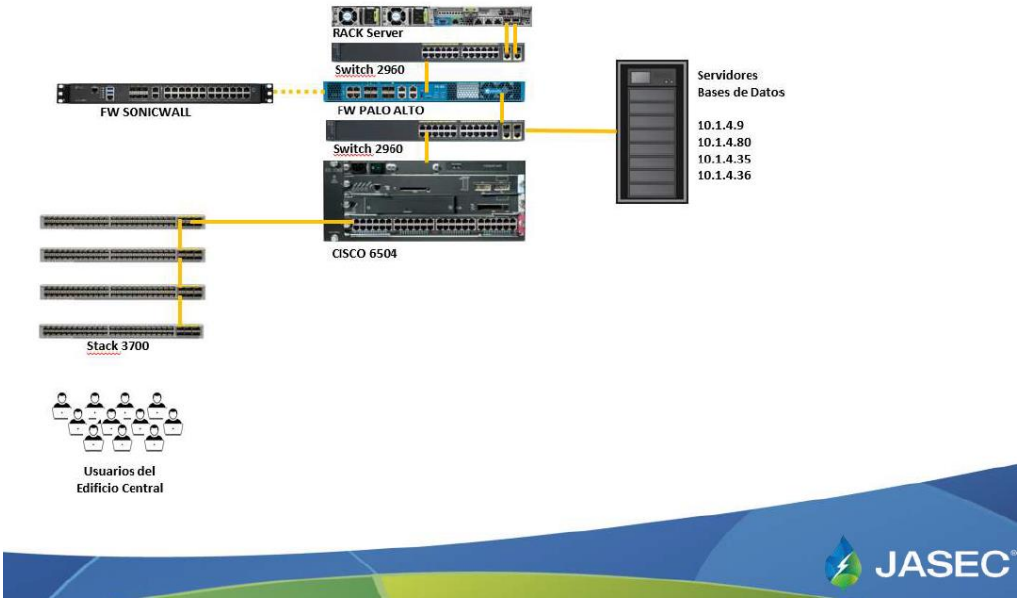
contratada para prestar el mantenimiento de los servidores, a ellos se les llamó y vinieron, hicieron una revisión y por dicha no se logró comprobar que las bases de datos fueron vulneradas o encriptadas, entonces esto nos dio una tranquilidad porque en caso de que las bases de datos estuvieran encriptadas o vulneradas si hubiera sido más crítico, a pesar que de eso sí habían respaldos la gente de bases de datos si nos garantizaron y nos aseguraron que habían respaldos, el proceso de recuperación hubiera tardado más, porque hubieran tenido que formatear los servidores, volver a montar los respaldos de las bases de datos, revisar que la información estuviera integra, porque no sabíamos inclusive si los respaldos de las bases de datos pudieran tener una amenaza, Conti no fue que entró el 21 de abril y el 22 atacó, no, se cree que Conti antes de concretar el ataque dura 6 meses adentro de la organización, ellos entran, investigan, validan accesos y cuando ya ellos llegan a un punto donde ya no pueden continuar sueltan la bomba, ya ahí es donde comienzan a encriptar, y ya la institución se da cuenta que fue vulnerada, entonces posiblemente JASEC tuvo ese virus desde hace 6 meses, antes de abril, pero, fue en abril cuando ya ellos hicieron toda la encriptación, se consultó si había contingencia o redundancia. Después de que se hizo toda la investigación y ya con un poco más de entendimiento de qué fue lo que había pasado, se decidió implementar una infraestructura limpia, ¿por qué una infraestructura limpia?, porque todo lo principal, ya todos los servidores estaban encriptados, el almacenamiento estaba encriptado, los Switchs posiblemente fueron vulnerados, los firewall estaban vulnerados, entonces qué había que hacer, teníamos que levantarnos desde cero otra vez, entonces qué se hizo, cuando pasó lo del ataque hubieron múltiples empresas que a mí me llamaron y me dijeron, mira si ocupas algo con mucho gusto, nosotros te ofrecemos ayuda, lo que ocupes con mucho gusto, pero a lo buen tico cuando ya se ocupa nadie puede, ahí se hicieron múltiples llamadas, yo conversé con una gente que fueron los que nos vendieron los fortines cuando yo estaba, conversé con Huawei, conversé con una empresa que se llama SisApp, conversé con Netway y muchos decían sí tenemos equipo pero está prestado, ahorita no lo tenemos, ¿por qué?, porque en ese momento no solamente JASEC se vio afectado, fueron muchas empresas (Ministerio) Hacienda, Ministerio de Trabajo, entonces

todas esas empresas que se encargaban de ofrecer tecnología, para ellos fue también crítico, porque todo mundo le comenzó a pedir; mira ocupo un equipo, ocupo una cosa, ocupo tal otra, ocupo restablecer, ocupo volver a levantar, entonces muchas empresas no tenían infraestructura para prestarle a JASEC, y ¿por qué prestarle? Porque JASEC no tenía un servidor para poderse levantar, los servidores que tenía estaban encriptados, no había un servidor para volver a levantar la infraestructura virtual, los servidores, osea volver a levantar todo desde cero, la única forma de hacerlo era que alguien nos prestará, entonces lo que se hizo fue que se consiguió un servidor físico digamos, obviamente lo suficientemente robusto, a nivel interno se consiguieron unos Switchs de comunicación y se encontró un Firewall pero Sonicwall no, yo no quise poner Sonicwall yo puse Palo Alto (Networks), porque yo dije mira sí, yo sé qué nivel global las marcas líderes son Check Point (software Technologies), Palo Alto (Networks) y Fortinet, toqué la puerta de Fortinet no tenemos equipo ahorita me dijeron, y si te podríamos prestar uno pero tendrías que comprarle la licencia, entonces en la situación en la que estábamos yo no tenía chance para ir y comprar una licencia, entonces Palo Alto (Networks) dijo yo te presto, pongámoslo a funcionar y así fue como empezamos……..



Señala el señor Martínez Picado que: a continuación, se detalla la infraestructura que inicialmente se montó, esos servidores de bases de datos son unos que ya había revisado la empresa, se montó un

servidor RACK ese servidor era igual como los de virtualización, tenía bastante memoria RAM, procesador y almacenamiento, y ahí comenzamos otra vez……



Continúa don Eddy Martínez indicando que: por instrucción de don Francisco (Calvo) se levantó primero facturación, lectura y cobro que era lo primordial, osea JASEC tenía que facturar y comenzar a cobrar sí o sí, ¿qué se hizo?, se volvió a montar todo desde cero, así fue desde cero, comenzar a montar los servidores virtuales, comenzar a configurarlos, crearlos, decirle a Osvaldo (Navarro) del departamento de sistemas que volviera a levantar los sistemas, vuélvalos a configurar, y ahí poco a poco, lo primero que se hizo fue como una burbujita, en el centro de datos tiramos un montón de cables y comenzamos a instalar servidores virtuales, a hacer pruebas, a nivel de redes hubo que volver a configurar todas las redes, le fuimos dando acceso poco a poco, primero este edificio, todo está funcionando bien, monitoreo, no se ven amenazas, virus, y no, ok, primero este edificio cuando ya estuvo listo, fuimos con el siguiente, y así fuimos uno por uno, lo vamos a ver más adelante, esto era mientras se reestablecía la infraestructura que fue vulnerada, que eran los cuatro servidores físicos y el almacenamiento, ¿por qué no se hizo primeramente en los 4 servidores?, porque nos hubiera tomado más tiempo, mientras que se restablecían los 4 servidores, se volvían a instalar, se volvía a montar el almacenamiento, todo nos

hubiera tomado más tiempo, en ese momento no teníamos tiempo, ocupábamos levantarlo lo más pronto posible pero de una forma segura, que no nos sucediera que tal vez estábamos levantando todo y “pum”, se nos metía Conti otra vez y todo para abajo y vuelva otra vez a levantarse, la idea era hacerlo de una forma segura, entonces por eso se hizo una burbujita……..

Hace ver que en las siguientes diapositivas se detallan todas las actividades que se hicieron:…..

Labores para la recuperación

- Revisión de los servidores de Bases de Datos (27 de abril)……
- Revisión y formateo de equipos de usuarios (06 de mayo-20 julio)……..
    - Edificio Central……..
    - Cerrillos……..
    - Paseo Metrópoli……
    - Fátima……
    - El Bosque……..
    - Barro Morado……
    - Birrís……...
    - Tuis……
    - Reconfiguración de la red……
    - Reinstalación de los equipos de core……
    - Subneteo……...
    - Listas de control de acceso (ACL’s)……..
- Implementación y configuración de firewall datacenter (03 de mayo)……
- Creación, configuración y hardening de servidores virtuales (04 mayo)……
    - Lectura, cobro y facturación……
    - Recaudación……
    - Sistemas de gestión internos……

- Configuración de políticas en el antivirus……..

- Recuperación de infraestructura de servidores virtuales (2022LA-000010-0018300001) 20 de junio…….
    - Recuperación de almacenamiento NetApp 2240……
    - Reinstalación de infraestructura Cisco UCS……
    - Reinstalación de Vmware……
    - Migración de servidores creados en infraestructura segura……
- Recuperación y configuración del almacenamiento Huawei (12 de julio)……..
- Recuperación y configuración del almacenamiento NetApp 2620……..
- Revisión y recuperación de información de carpetas compartidas (18 de julio)……..
    - Revisión respaldos de información que no se encuentran encriptados……
    - Copiado de información limpia en servidor virtual……..
- Recuperación de infraestructura de escritorios virtuales (05 de agosto)……
    - Reinstalación de Vmware……
    - Creación, configuración y hardening de servidores virtuales……
    - Creación, configuración y hardening de escritorios virtuales……..
    - Actualización de firmware thin clients……
    - Inclusión de planes de inversión ante la Comisión Nacional de Emergencias……..

Primeramente se revisaron los servidores de base datos, vino la empresa nos corroboró y mediante un informe, ellos nos hicieron un informe y nos dijeron las bases de datos están limpias, pueden estar seguros de que están limpias, las conectamos, se conectaron los sistemas, probamos la conexión de los sistemas con las bases de datos, se vio que si conectaba, se verificaron e hicieron consultas, levantamos cobro y se vio que si conecta, se consultó un número de abonado y salió que debía tanto, okay, entonces una vez hecho todo esto, no nos podíamos jugar el chance de si una máquina de un usuario estaba contaminada o no, ¿por qué?, porque ya en plataforma habíamos visto una máquina

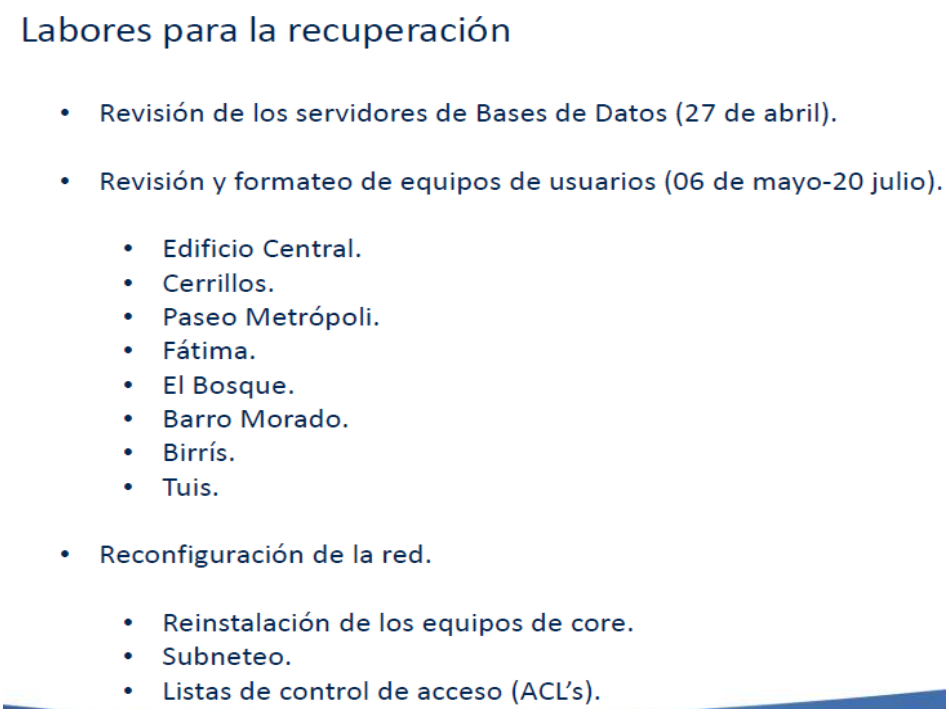
contaminada, la máquina estaba encriptada, tenía archivos encriptados, entonces no podíamos saber a ciencia cierta, si había alguna otra máquina más contaminada, ni tampoco podíamos darnos el lujo de volver a levantar todo, conectar las máquinas a la red, y si la máquina tenía un virus nos iba a traer todo abajo, ¿qué hicimos? Se formateó todo, entonces TI como decimos se "enrolló las mangas" y procedió a formatear, hicimos todo un procedimiento para formatear, se instaló Windows 10 porque Windows 7 ya estaba fuera de mercado ya Microsoft no le daba soporte, y ¿qué pasa con las máquinas que no tenían licencia de Windows 10?, así se va, ya después pensaremos en cómo comprar las licencias, pero por el momento ocupamos levantar rápido, de una forma segura, las maquinas se parcharon, se les instalaron todas las actualizaciones, se le instaló el antivirus correspondiente, se le instaló una solución que el mismo MICITT (Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones) recomendó que era el microCLAUDIA, ese el MICITT se lo dio a todas las empresas que fueron atacadas, esa es una solución que lo que hace es detectar si la maquina tiene ransomware por medio de una consola principal la gente de TI revisa si hay una máquina comprometida o no, entonces todas las máquinas debían tenerlo, ese fue el orden que se siguió Edificio Central, Cerrillos ¿por qué Cerrillos?, porque por medio de Cerrillos es donde se interconecta por fibra todos los edificios, osea Fátima llega a Cerrillos primero y luego aquí, el Bosque llega a Cerrillos primero y luego, Paseo Metrópoli primero llega a Cerrillos y después aquí, entonces por supuesto que teníamos que habilitar primero Cerrillos ahí igual se revisaron y se formatearon las maquinas, se habilitaron los sistemas posteriormente Paseo Metrópoli para que la gente pudiera ir a pagar ahí, después Fátima el más grande que ahí tuvimos un atraso muy grande, que tal vez don Francisco (Calvo) si quiere lo explica…….

Interviene don Francisco Calvo para indicar que: en Fátima la situación que tuvimos es que en este momento todavía estábamos en teletrabajo, y uno de los efectos que tuvimos con el teletrabajo era que la gente no quería volver a trabajar a las oficinas, entonces para hacer ese proceso que explica Eddy (Martínez) se ocupaba que la gente viniera, realmente hubo resistencia, ese es un subproducto o un efecto de haber implementado en su momento el teletrabajo como medida en emergencia, pero en el

fondo eso demuestra de que muchos de los que entramos a trabajar no estaban aptos para teletrabajo, entonces eso fue parte del atraso que tuvimos en ese momento, también quiero aprovechar para explicar por qué sobre todo al inicio el tema de la estrategia que se tomó, dado que la prestación del servicio propiamente no fue afectada lo siguiente más importante que teníamos que recuperar era la minita de esa plata, es decir, ¿Cuál es esa parte central? Es dado que estoy dando servicio eléctrico, y dado que estoy dando servicio de internet lo que necesito es poder leer, facturar y cobrar, eso es lo primero que había que poner a andar antes que la Contabilidad, antes que el presupuesto y antes que todo lo demás, porque si yo no tengo recursos luego no voy a poder pagar planilla, pagar los bancos, me van a cobrar intereses, pagarle a los proveedores, etcétera, y luego si a los clientes se les acumulaban muchos recibos no iban a tener plata para pagar, e iba a hacer todavía más grande el problema del atraso en los pagos de las facturas, entonces ese era el foco principal, poder generar recursos para luego poder reutilizar y no generar una acumulación muy grande de recibos, ese es el foco de la estrategia que se inició y a partir de ahí ya poder recuperar el resto de los sistemas e infraestructura que Eddy (Martínez) va a explicar, pero esa era la razón principal, si empezábamos por otro lado en realidad no nos iba a ir bien, íbamos a morir antes de llegar a ese punto……..

Resalta don Eddy Martínez que: así se continuaron los demás edificios, posteriormente se revisó y se instaló el Bosque, Barro Morado y ya de último Tuis, y de hecho esa etapa de formateo concluyó el 20 de julio e inicio el 06 de mayo, prácticamente duramos casi 3 meses con las máquinas, ahí, más que todo era los compañeros de soporte, ellos son los que formatearon prácticamente que todos los equipos. También se realizó una configuración a nivel de red, se formaron los equipos Core, los equipos principales de comunicación de cada edificio, ellos se formatearon, se reinstalaron, se hizo una reconfiguración a nivel de las redes; para que me entiendan antes este edificio, antes del ataque tenía una misma subred, todo mundo estaba en la misma red, en este edificio digamos, posterior a esto ya no puede ser así, entonces ahora digamos Plataforma es una red, Facturación es otra red, Soporte es otra red, Comercial es otra red, Gerencia es otra red, y así por cada uno de los edificios igual en Fátima que

Tesorería es una red, Contabilidad es otra red, y esto ¿Por qué? Porque si por X o Y razón el día de mañana llega a meterse una amenaza, está solamente se va a contener es esa pequeña red que hay, no se va a transferir o comunicar con otras subredes, también se configuraron las famosas listas de control de acceso las cuales les indicaba anteriormente que no habían, ya ahora el muchacho de comunicaciones, ya él configuró la parte de los ACL´s , eso lo que permite es que solamente le permite a usted comunicarse con un destino específico, no hay de otra, entonces digamos si por ejemplo; la subred de plataforma se quiere comunicar con Gerencia no va a poder, porque Plataforma solo tiene derecho a conectarse a X, Y, Z y listo, eso a nivel interno, obviamente a nivel perimetral hay otra configuración y todo lo demás……..



De igual forma se hizo la configuración e implementación del Firewall de Palo Alto, pero este firewall ya no funge como firewall perimetral, sino que ahora funge como Firewall de Data Center, esto qué quiere decir, que cualquier máquina que quiera ir a los servidores virtuales, al almacenamiento, a las bases de datos primero tiene que pasar por el Firewall, antes no había eso, antes cualquier persona de aquí podía acceder a los servidores a la libre, no había restricción alguna y posteriormente ya se hizo la creación

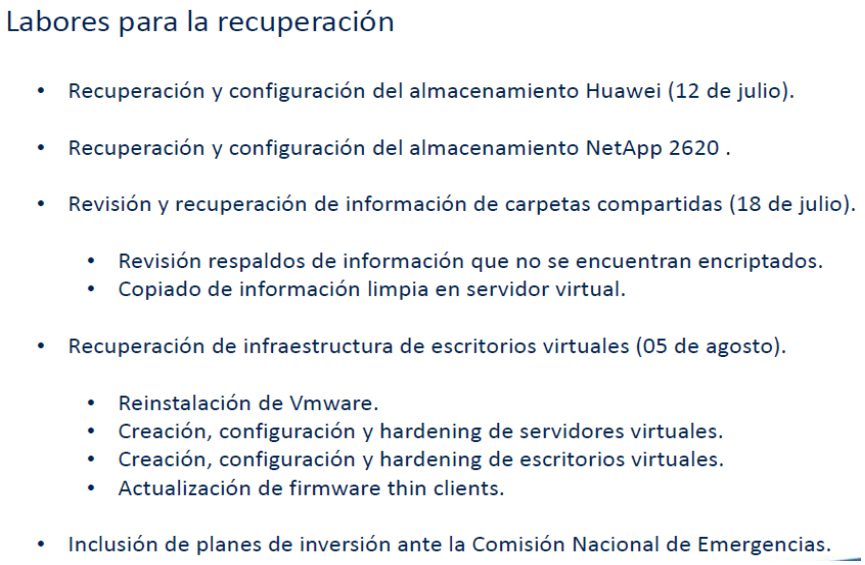
de los demás servidores virtuales que habían los de recaudación, los sistemas internos, algunos otros sistemas como el de Auditoría, SIFAJ, Recursos Humanos y en algunos otros sistemas, eso sí se trabajó en conjunto con don Francisco (Calvo) para ir definiendo prioridades, de todos los sistemas que habían antes se hizo una priorización, de los ciento y resto de servidores virtuales que habían antes, se determinó el contenido de cada uno y de eso se hizo una priorización y esos fueron los que se iniciaron a configurar y a crear. Se cambiaron las políticas del antivirus, como les indicaba se bloquearon los USB´s porque durante el levantamiento tuvimos un incidente, una máquina conectó una llave maya y nos contaminó la máquina, tenía 53 virus la máquina entonces esa máquina evidentemente tuvimos que formatearla otra vez, y de ahí se tomó la decisión de bloquear los USB´s, nadie puede utilizar USB´s ni discos duros, ni llaves mayas, solamente se permite el mouse, el teclado, la firma digital y alguna que otra impresora. Después de esto se sacó contratación que fue para toda la recuperación de toda la infraestructura que fue vulnerada, ahí son los almacenamientos, NetApp, los servidores, Cisco, se reinstaló el Vmware que es el software con el que se administra toda la solución de virtualización, y una vez que eso ya estaba listo se migro todos los servidores que habíamos creado en el servidor que nos habían prestado, y ya una vez que esto estaba seguro, configurado y asegurado se comenzó a migrar todo de aquí para acá, se comenzó a migrar y a migrar, y ya una vez que tuvimos más recursos se terminó de configurar todo los demás servidores que eso es a la actualidad…….

Labores para la recuperación

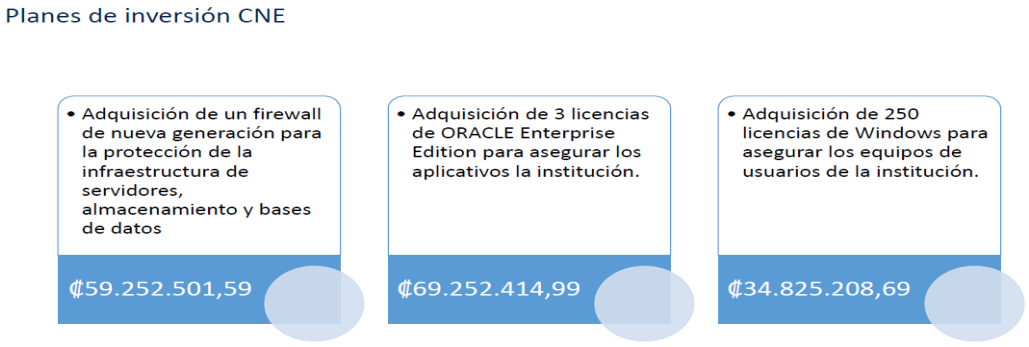
- Implementación y configuración de firewall datacenter (03 de mayo).
- Creación, configuración y hardening de servidores virtuales (04 mayo).
  - Lectura, cobro y facturación.
  - Recaudación.
  - Sistemas de gestión internos.
- Configuración de políticas en el antivirus.
- Recuperación de infraestructura de servidores virtuales (2022LA-000010-0018300001) 20 de junio.
  - Recuperación de almacenamiento NetApp 2240.
  - Reinstalación de infraestructura Cisco UCS.
  - Reinstalación de Vmware.
  - Migración de servidores creados en infraestructura segura.

Continúa don Eddy Martínez indicando que: ahí durante todo ese proceso de recuperación, obviamente como yo les indicaba la Huawei fue encriptada, le solicitamos ayuda a la empresa que vendió el Huawei, pero no quiso más bien nos cobró como $5000 para venir a reinstalar, entonces le solicitamos ayuda directamente al fabricante, a hoy nosotros en Infocomunicaciones tenemos muy buena comunicación con Huawei, entonces nosotros le pedimos ayuda Rodolfo (Sanabria) principalmente, y vino un técnico de Huawei directamente, él vino, revisó y nos corroboró que no estaban configurados los respaldos de la Huawei en los servidores virtuales, la volvió a reinstalar, la pusimos otra vez a andar y ya quedó totalmente funcional, pero antes de eso también se reconfiguraron los dos NetApp, digamos los dos otros almacenamientos que antes estaban en TI, justamente en este proceso de recuperación uno de los NetApp colapsó y se quemó, el no arranco más, y era el que estaba justamente fuera de garantía por eso se iba a comprar este otro almacenamiento porque ese ya no tenía soporte, sabíamos que en cualquier momento él iba a llegar y no iba arrancar, y así sucedió no arrancó más, entonces está ahí, ahí lo tenemos para ver qué vamos hacer con el porque los discos duros están buenos, ese almacenamiento tiene 24 discos de 2 Teras, es decir, tiene 48 Tera y es una lástima botar los discos, ya que prácticamente lo que está malo es la controladora, entonces vamos a ver de qué forma se restaura la controladora o se compra una controladora nueva para ponerlo a funcionar. Durante ese proceso también se revisaron las carpetas compartidas, ahí por dicha a pesar de que la información de las carpetas compartidas fue encriptada ahí si teníamos respaldos, entonces se hizo todo el proceso de recuperación de los respaldos, habían unos respaldos que estaban encriptados, pero habían otros que no lo estaban entonces tuvimos la suerte de que la información de las carpetas estaban una semana antes del ataque y estaba limpia, entonces ahí se hizo la migración o la extracción digamos de la información de las carpetas compartidas, se le dio a TI para que posteriormente volviera a comenzar a crear la infraestructura de servidores de carpetas compartidas y copiará la información que estaba antes, y también se volvió a recuperar toda la infraestructura de escritorios virtuales, pero ya aquí no se permite que las personas que tengan escritorio virtual lo accedan desde fuera de la red de JASEC, osea desde

internet, ya no pueden conectarse, eso no se habilitó solamente se habilitó a nivel interno, ahí se configuraron otra vez los servidores virtuales que administran la solución de virtualización de escritorios, se volvieron a configurar los escritorios virtuales igualmente en Windows 10, se hizo una actualización del sistema operativo de los thin clients, estos son equipos tontos, no tienen disco duro, no tienen nada, simplemente fungen como un medio de interconexión entre el usuario y el servidor central nada más, se actualizó el firmware y ya están operando, ahí durante todo este proceso como mencionaba anteriormente el Gobierno había declarado un estado de emergencia, y nos tomaron en cuenta a nosotros para lo de la Comisión Nacional de Emergencia, eso lo estaba llevando don Guillermo (Gómez), pero posterior a la salida de él, lo llevé yo……



Hace ver don Eddy Martínez que: ahí don Guillermo (Gómez) había metido 3 planes de inversión a nivel de la Comisión Nacional de Emergencias, y que son los que se muestran en la siguiente diapositiva:…….



El primero sobre la adquisición de un firewall perimetral, que va a fungir como firewall de Data Center en lugar de Palo Alto que está ahorita funcionando, tres licencias de Oracle, ¿por qué licencias de Oracle?, porque hay muchos sistemas que están desarrollados por personas de aquí, por el departamento de Osvaldo (Navarro), pero están en una versión muy vieja de Oracle, y justamente eso corre solo en versiones muy viejas de sistemas operativos, entonces cuando se restableció toda la infraestructura de servidores virtuales todo es Windows server 2022 y 4 servidores del 2019, adicionalmente dentro del plan de inversión se solicitaron 250 licencias de Windows para todos esos equipos que se instalaron en Windows 10 y que no tenían licencia Windows 10 porque tenían licencias Windows 7, pero ese la Comisión Nacional de Emergencias no la aprobó, dijo que ellos no veían cuál era la relación del ciberataque con las licencias de Windows, entonces esa no la aprobaron, pero sí nos aprobaron las dos primeras, esa es una donación, de hecho ya se mandaron los requerimientos técnicos a la Comisión Nacional de Emergencias, de hecho creo que el lunes viene el especialista en seguridad que contrató la Comisión Nacional de Emergencias para que él sea el fiscalizador de las contrataciones, yo pude observar un poco lo que metieron las otras organizaciones y todo mundo metió Firewalls, algunas licencias de Oracle, metió soluciones de EDR que eso es protección especializada a nivel de los equipos, es como un adenda que se le hace al antivirus para que tenga la protección de ransomware. Interviene don Francisco Calvo para indicar que: con respecto al tema de la Comisión Nacional de Emergencias, si bien es cierto nos participaron y se llenó toda la tramitología, etcétera, al final hubo que ir a defenderlo, verdad Eddy (Martínez), hubo una sesión de la Junta Directiva de la Comisión Nacional de Emergencias, Eddy (Martínez) y yo fuimos, y al final invertimos toda una mañana, y aunque al inicio fue como muy fácil más bien luego nos volvieron a llamar y hubo que hacer una defensa fuerte, porque digamos que no era algo automático, entonces si bien es cierto hubo un plan que no aprobaron es el plan menos costoso o menos cuantioso, los otros 2 que realmente eran más cuantiosos por dicha se logró que se aprobaran, pero sí hubo que hacer un proceso de defensa en mi caso más de estrategia, en el caso de Eddy (Martínez) más técnico pero si costo un poquito para lograr esa aprobación. Otro

aspecto en este caso es que son recursos no reembolsables, y luego que por dicha nosotros no compramos, sino que son ellos los que compran y nos dan, así nos liberamos de todo ese proceso engorroso, y por decirlo así el tema de la liquidación o de la rendición de cuentas es más sencilla, porque al final de lo que tenemos que rendir cuentas es de que lo que recibimos se instaló y está funcionando, más no el uso de recursos, que es muy complejo y a veces muy peligroso, entonces ese esquema nos parece muy bien porque es más sencillo y menos riesgoso para nosotros……

Resalta don Lizandro Brenes que: ya se acabó la hora de presentación, pero a mí me parece que sería imprudente no terminar la presentación de don Eddy (Martínez) por la importancia del tema, entonces como faltan 12 filminas más o menos que es como una tercera parte de la presentación, más o menos el tiempo sería de 30 minutos más, y a mí me parece que sí deberíamos dejar que la Administración termine el informe y posponer la discusión para la siguiente sesión, con el fin de que podamos terminar la presentación, y obviamente sí tener la discusión que tenemos que tener pero no forzada ni a la carrera, sino una vez que nos hayan presentado la información y después ya abordarlo, entonces esa sería mi propuesta, no tener la discusión hoy sino que antes terminen ellos de exponer en esos 30 minutos que quedan……

Procede la Presidencia a someter a votación, para alterar el orden del día, o más bien ampliar el tiempo de discusión y que la Administración pueda terminar la presentación, serian 30 minutos más y posponer la discusión para la siguiente sesión. Si están de acuerdo pueden levantar la mano; resalta que se tienen 7 votos a favor, quienes estén de acuerdo con la firmeza por favor que levente las mano; hace ver que tenemos 7 entonces queda aprobada la moción de manera unánime y en firme con 7 votos de los que estamos acá, entonces con toda la tranquilidad se puede continuar con la presentación……

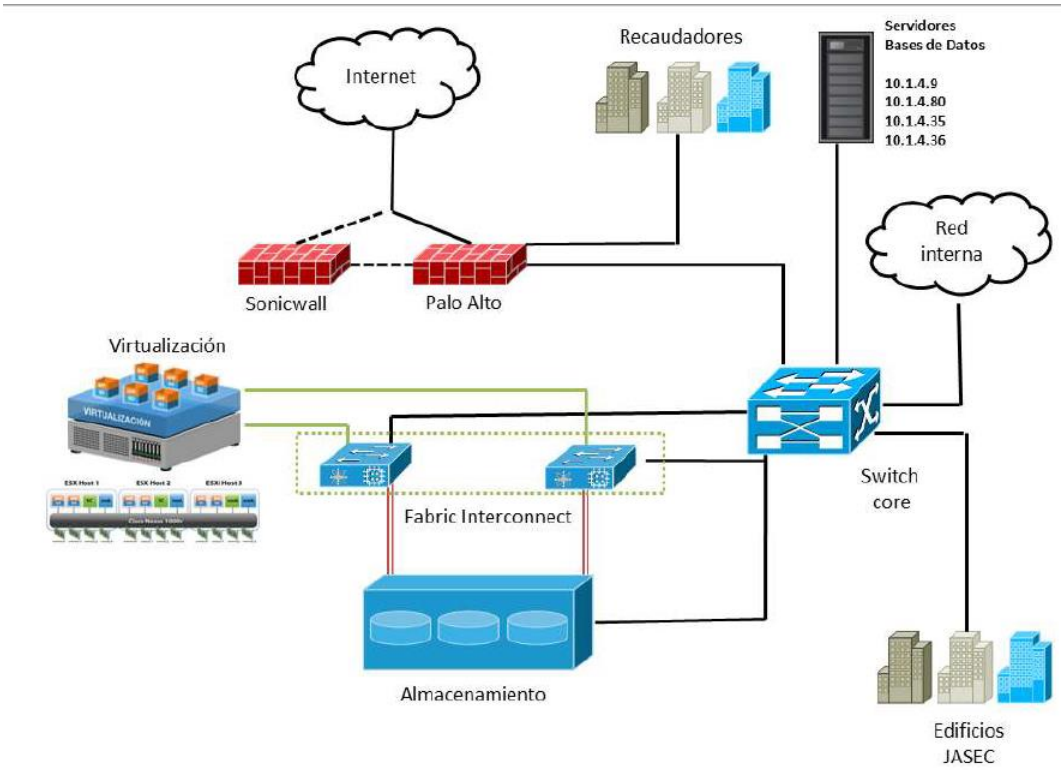
SE ACUERDA: de manera unánime y afirmativa, con siete votos presentes……

Ampliar la duración de la sesión hasta por 30 minutos más……....

……..

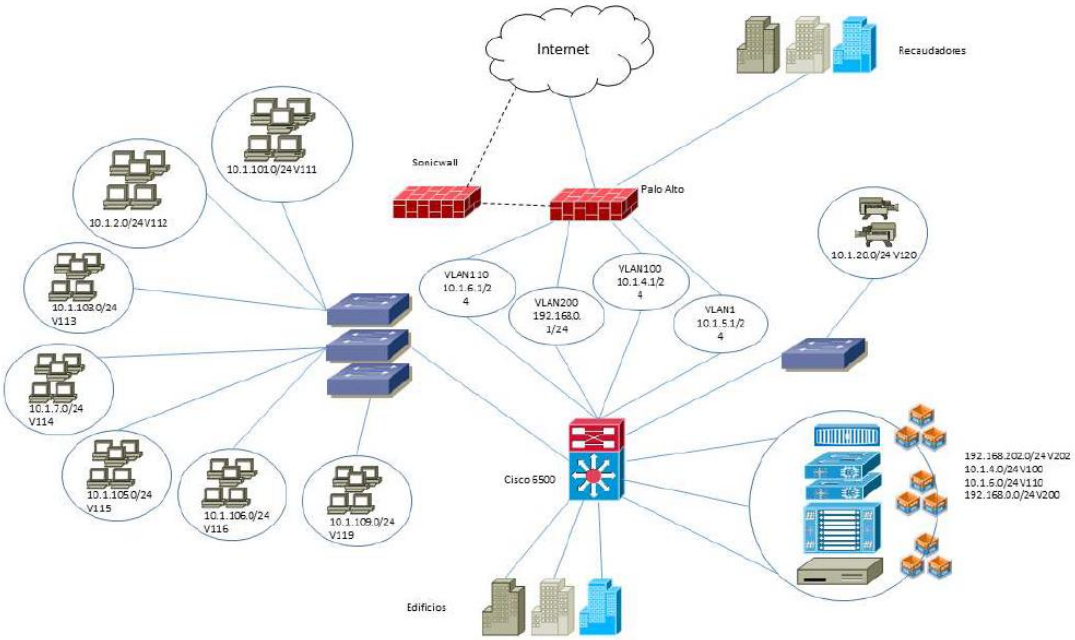
……..

Continúa don Eddy Martínez la presentación indicando que: está es la situación a cómo estamos ahorita:.



A pesar que tal vez ustedes digan que es muy similar a lo que estaba anteriormente, pues sí es muy similar a lo que estaba anteriormente, antes del ataque pero a nivel físico, a nivel lógico ha cambiado mucho, ya a nivel lógico tenemos las listas de control de accesos en el Switch Core, ya no están los Sonicwall ahora está el Palo Alto (Networks) entonces hay bastante confianza, tiene mayores características configuradas, es un firewall de Data Center, también funge actualmente como hardware perimetral, los recaudadores pasan a través del mismo firewall, hay una configuración más detallada, se hizo una configuración más granular, ya no es como estaba antes, que cualquier cosa se comunicara con cualquier cosa, se fuera por cualquier puerto, ya no es así, a nivel también de la solución de virtualización se instaló la última versión soportada por los equipos que es la versión 6.7 de Vmware, se eliminaron los 2 equipos MDS que estaban en el diagrama anterior, todos los edificios tienen que pasar por el firewall Data Center para poder conectarse a cualquier base de datos, a cualquier cosa que esté dentro del Data Center, y ahí también están configurados los otros 2 almacenamientos que es el NetApp que es donde estaban las carpetas compartidas, y el Huawei……

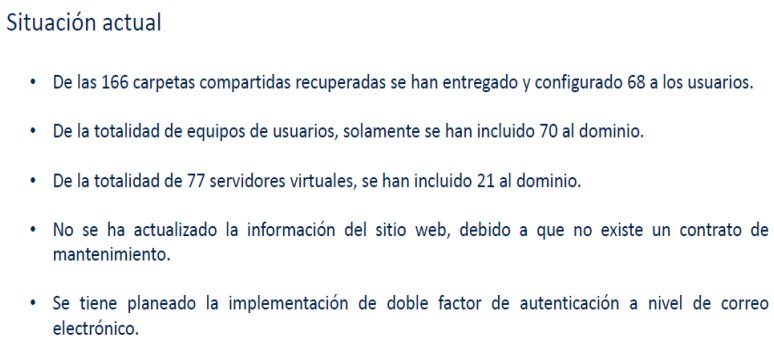
Indica don Eddy Martínez que: la imagen anterior mostraba un diagrama físico, pero a nivel lógico está y como se muestra en la siguiente diapositiva:……...



En la configuración lógica Palo Alto tiene 4 redes o subredes configuradas que son las que protege, a bueno eso es otra cosa, las subredes se cambiaron, ya no es el mismo direccionamiento que había antes, es muy lógico que sí fuimos atacados no debemos poner las mismas IP´s que teníamos antes, tenemos que cambiar completamente el direccionamiento IP, ya los servidores no tienen el mismo direccionamiento que antes, los usuarios no tienen el mismo direccionamiento que antes, solamente los servidores de bases de datos se quedaron con las mismas IP´s porque cambiarlos conllevaba a prácticamente volver a cambiar los sistemas, todos, ya que casi que todos comunican a través de la dirección IP de las bases de datos, fueron los únicos servidores que mantuvieron las IP´s, pero todo el resto todo se cambió. A nivel lógico esa es la configuración, hay 4 subredes que protege el Sonicwall y a nivel de usuarios el direccionamiento es diferente, todas las subredes de los distintos edificios se manejan en el Core principal, antes no, antes las subredes estaban configuradas aquí y se pasaban de aquí a Fátima, pero ya no, ya cada edificio tiene su subred declarada en cada Switch central……...

……..

Del total de carpetas compartidas, según me indica la gente de soporte ya se han entregado 68 carpetas compartidas y ya los usuarios las utilizan, de los servidores que se han logrado levantar dentro de ellos está un servidor del active directory que es donde se meten todas las máquinas en el dominio y que todos estén es un solo dominio. De la totalidad de equipos JASEC tiene aproximadamente 400 equipos, 350-400 equipos de los cuales solo se han incluido 70, de la totalidad de los 77 servidores que se han creado a la fecha hay 21 incluidos en el dominio, posterior al ataque el sitio web no se está actualizando, mucha información del sitio web se perdió, no había respaldo de esa información, nadie actualmente le está dando mantenimiento al sitio web, no hay contrato con una empresa que les brinde mantenimiento, se tiene implementado habilitar la autenticación de doble factor a nivel de correo electrónico, eso es que los usuarios entren con un usuario y la clave pero que a la vez tengan un token para poder entrar, eso hace más difícil el hackeo de correo electrónico……



Continúa el señor Martínez Picado que: sobre lo que está pendiente, obviamente ver la viabilidad y la posibilidad si es factible verdad, obviamente por un análisis forense, sobre si es posible hacerlo sino hay evidencia actualmente y pues no tiene ningún sentido hacer un análisis forense, concluir la entrega de las carpetas compartidas eso le corresponde a la gente de soporte, incluir obviamente la totalidad de las máquinas al dominio puesto que solamente hay 70, realizar la actualización del sitio web, ahí a nivel de sitio web habían algunos módulos, principalmente de SWF para que las personas pudieran consultar su factura eléctrica, habilitar el doble factor de autenticación……

……..

Pendientes

- Ver la posibilidad y viabilidad de efectuar un análisis forense.
- Concluir la entrega de las carpetas compartidas.
- Concluir la inclusión de la totalidad de los equipos al dominio jasec.go.cr, tanto a nivel de equipos de usuarios como a nivel de servidores virtuales.
- Realizar la actualización de la información del sitio web de JASEC, así como analizar el riesgo de habilitar nuevamente el SWF y la consulta de recibos eléctricos y de internet.
- Habilitar el doble factor de autenticación a nivel de correo electrónico.
- Instalar el licenciamiento de Windows Server para la infraestructura de servidores que se solicitan en la Licitación Abreviada 2022LA-0000017-00183.

Adicionalmente a la contratación de restablecimiento de los servidores se hizo otra contratación que es para comprar la licencias de Windows que nos faltaban, por qué toda la infraestructura de servidores virtuales se levantó sin licenciamiento Windows, JASEC no tenía licencia de Windows 2022 que son todas las licencias que se compraron, mediante esa contratación se compraron las licencias de Windows, también se compró la renovación del soporte del NetApp que no estaba el soporte del NetApp, se compró el soporte de los equipos que administran la virtualización, esos no tenían soporte, no había soporte de Cisco, eso se metió en la contratación, el alquiler del Palo Alto mientras que la Comisión Nacional de Emergencias hace la compra y nos dona el equipo, ¿Por qué Palo Alto?, bueno primero como lo pudieron ver según Gartner es una de las marcas líderes a nivel mundial, y ¿Por qué se va a comprar un Palo Alto?, porque no tiene mucho sentido si yo tengo un Palo Alto aquí comprar otra marca y volver a configurar todo desde cero otra vez, entonces la idea es seguir conservando el Palo Alto, cuando ya la Comisión Nacional de Emergencias compre Palo Alto y lo done, es simplemente pasar la configuración de este equipo al otro equipo, y todo queda funcionando como está ahorita……. Adiciona que cuándo pasó el ataque Microsoft nos ofreció a nosotros 6 meses de Office 365, dentro de esos seis meses fue cuando se emigró el correo a la nube, pero los seis meses vencieron en octubre, entonces se tuvo que tomar la decisión de si continuamos con Office 365 o volvíamos a la solución de correo que teníamos antes, por temas presupuestarios comprar Office 365 es cariñoso muy caro,

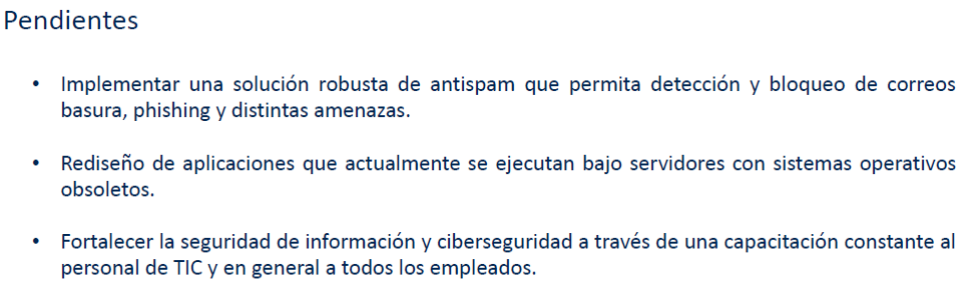
principalmente porque no es solamente el Office digamos, atrás de eso va una serie de características que vende Microsoft, al final Julio (Quesada) hizo un estudio, y una comparación y una recomendación en la que dijo que por temas presupuestarios se recomienda que se siga manteniendo el mismo servidor de correo electrónico que había antes del ataque, y ese es el que está ahorita, está otra vez aquí en la infraestructura de JASEC, ya no está en nube como estaba antes, entonces no se continuo con Office 365, y en el almacenamiento se configuraron los respaldos ahí yo le indique a Egon (Hernández) que se cerciorara que realmente estuvieran los respaldos, y él me dijo que sí que lo respaldos realmente sí están, entonces pues ahí sí tenemos respaldados los servidores virtuales, inclusive validamos con el mismo técnico de Huawei que nos ayudó a configurar y a restablecer el almacenamiento, él entró y lo revisó y me dijo que sí que ya estaba, si pasara algo ya tenemos al menos un respaldo, que Dios quiera que no. Luego hay otro asunto muy importante, los servidores, los 4 Blade, los cuatro servidores físicos que son los que administran la solución de virtualización ya a partir del año pasado no tienen soporte del fabricante, entonces ahí se tiene que invertir en comprar esos servidores nuevos, porque si algo sucede no hay soporte con Cisco, entonces sí es muy importante que lo tomen en cuenta, no sé si soporte lo metió en el presupuesto, esos vencieron el año pasado, son funcionales y pueden seguir funcionando, y no es que no tengan respaldo, es que no tienen soporte del fabricante, es decir, si en este momento un equipo de esos se apaga nadie sabe cómo poderlo restablecer, salvo el fabricante, pero como no hay soporte con el fabricante entonces no se puede arreglar, esa es la importancia, la ventaja es que como esos equipos son funcionales realmente se pueden reubicar en otro lado, se pueden reubicar en un sitio alterno por ejemplo, se pueden mandar a Infocomunicaciones, de Infocomunicaciones al Data Center y ahí está el respaldo. De igual forma justamente lo que mencionaba, sobre adquirir una solución de sitio alterno, para los servidores virtuales, y principalmente para las bases de datos que es lo más lo más crítico. También está pendiente la implementación de una solución para protección de ransomware que eso es lo que menciona ahí, una solución de EDR o NDR cualquiera de los 2, eso ayudaría a reforzar la protección a nivel de la red interna y los equipos de usuarios……..

Pendientes

- Adquirir el licenciamiento de Windows 10 para los equipos de usuarios que fueron formateados y que anteriormente tenían Windows 7.
- Efectuar la renovación tecnológica de los 4 servidores Blades que conforman la infraestructura de virtualización, los cuales no tienen soporte desde diciembre del 2021.
- Adquisición de un equipo de seguridad firewall lo suficientes robusto que brinde una seguridad a nivel de la capa de datacenter.
- Verificación y aprobación de la renovación del soporte solicitado en la Licitación Abreviada 2022LA-0000017-00183.
- Adquirir una solución de sitio alterno que contemple los servidores virtuales y Bases de Datos.
- Implementar una solución de EDR o NDR para reforzar la protección y seguridad de la red interna.

Hace ver don Eddy Martinez que: también es muy importante implementar una solución de anti spam, a pesar que el servidor de correo tiene un anti spam, pero es muy básico, hay soluciones de anti spam más robustas, por ejemplo; la misma gente de Sophos, ellos tienen una solución muy robusta de anti spam, entonces sí es muy importante adquirir una solución de anti spam, principalmente para que no vuelva a suceder lo mismo, que tal vez de pronto vaya a entrar algún archivo adjunto por medio de un correo, ustedes saben que a nivel de seguridad informática el eslabón más débil es el usuario, así es, entonces si los usuarios no están bien conscientes de la amenaza, y lo que acaba de pasar nos va a seguir pasando lo mismo. De igual forma hay que hacer un rediseño de aplicaciones que actualmente se ejecutan bajo servidores de sistemas operativos, esto se resuelve con las licencias de Oracle que nos va a comprar la Comisión Nacional de Emergencias porque es una versión más nueva de Oracle, entonces la gente de Osvaldo (Navarro) o la gente de sistemas lo que va a tener que hacer es recopilar todos esos sistemas que están en una versión muy vieja de Oracle, y pasarlos a la nueva versión de Oracle, entonces con esto obviamente vamos a eliminar muchas vulnerabilidades que justamente tienen esa versión vieja que tiene Oracle. Y obviamente, como lo acabo de decir que el eslabón más débil es el usuario, hay que hacer una capacitación muy fuerte a nivel de seguridad informática, a nivel de todos los usuarios, no solamente a nivel de TI, sino de todos los usuarios, para eso existen plataformas,

herramientas, charlas, en realidad hay mucho material en internet para concientizar a los usuarios sobre la importancia de la seguridad informática, y lo que puede llegar a pasar si alguno de ellos, y no es que lo haga adrede, tal vez no conoce, ya que para un usuario si yo le llevo un archivo adjunto de Word y el piensa que es un archivo válido de Word y lo abre y tal vez no es así…….



Indica el señor Martínez Picado que: durante el proceso del ciberataque ahí se hizo una versión económica, las dos contrataciones evidentemente, que una es el restablecimiento físico de la infraestructura virtual, que es volver a recuperar toda la infraestructura que fue vulnerada, servidores, almacenamiento, los Switchs de fibra canal, la compra de las licencias de Windows, que son las licencias de Windows, la renovación del soporte de Cisco, la renovación del soporte del NetApp de almacenamiento, y el arrendamiento del Palo Alto por 4 meses, para volver a restablecer el servidor de correo electrónico se contrató a una empresa para que volviera a configurar e implementar el Kerio, luego la implementación y configuración del Qwizard, ese es el sistema de colas que utiliza Hugo (Murillo) en plataforma, porque antes todo se hacía manual, entonces la empresa cobro $361.60 para volver a habilitar la plataforma. También cuando se cayó toda la central telefónica se le contrató a una empresa para que pudiera funcionar una central lastrics que tiene Julio (Quesada), y la última línea de la tabla corresponde a un servicio que se paga en Microsoft Azure que es por el DNS público, eso es para poder publicar a Internet el correo electrónico y la página web, que son los dos servicios que hasta el momento están publicados a internet……..

……..

……..

Costos

Descripción	Costo
Licitación Abreviada N° 20222LA-000010-0018300001 "Restablecimiento físico y virtual de la infraestructura de servidores y monitoreo de seguridad".	$50,850,00
Licitación Abreviada N° 20222LA-000017-0018300001 "Licencias Windows, arrendamiento sin opción compra".	$48,083,34
Implementación y configuración de Kerio Connect.	¢4.288.350,00
Implementación y configuración de Qwizard.	$361,60
Configuración de Central telefónica Asterisk, como medida de contingencia y provisional.	¢226.746,93
Servidor DNS público en Microsoft Azure.	$34,32

Finaliza don Eddy Martínez indicando: eso sería todo de mi parte……..

Externa don Lizandro Brenes: muy bien, a mí me gustó mucho la dinámica de la presentación, porque atiende el qué, cómo y cuándo, también le agradezco muchísimo la transparencia porque también estamos diciendo qué había, que se encontró, que se debe hacer, entonces muy bien vamos a continuar con la sesión, así te puedes ir un poco más temprano, pero lo vamos a requerir en próxima sesión, o en próximas sesiones ahí con don Francisco (Calvo) nos ponemos de acuerdo, porque inclusive a partir de esto hay algunos temas que debería abordar la Junta Directiva no solamente la explicación del ciberataque, sino decisiones que eventualmente se tendrían que tomar. Muchas Gracias……

Comenta don Lizandro Brenes que: se tenía una propuesta de acuerdo que estaba alineada para ser vista después de la discusión, entonces aquí la moción sería, posponer la discusión de este tema para una próxima sesión……

Interviene don Alexander Mejías para indicar: yo quería proponer algo más, que tal vez entre todos podríamos hacer una serie de preguntas porque son muchas, entonces tal vez ponernos de acuerdo de aquí al martes-miércoles, hacer una lista de preguntas y dárselas a la Administración……..

Externa doña Rita Arce: yo preferiría que las mías si mes las contestaran una por una, porque en otras ocasiones ya he mandado oficios y oficios y (…)……..

Comenta el señor Mejías Zamora que: la propuesta era tal vez poner como un repositorio, entonces yo pongo las mías, y si usted ve que dentro de las mías no concuerdan con las suyas usted pone las suyas,

como para entregarle una serie de preguntas a la Administración y en la siguiente sesión dedicarnos a escuchar las respuestas……

Externa don Salvador Padilla: a mí no me parece mal, sin embargo es que la deliberación y discusión de temas de este tipo, y la interacción que debe de haber con las personas a cargo de las investigaciones, me parece que el ejercicio de la deliberación, el debate y la discusión son sanos a nivel de una Junta Directiva, entonces yo no querría que eso se perdiera por una cuestión de nada más de enviar un listado y que nos respondan, sino que haya ejercicio de pregunta y respuesta, es decir, mientras no se pierda ese ejercicio yo creo que se pueden prever preguntas, cada quien las puede llevar amparadas, pero que también eso no impida que alguien pueda interactuar en el momento, yo creo que eso es válido e importante también, acorde a la discusión que se vaya a manejar, porque puede ser que nos vayamos por un lado donde la discusión pueda irse ampliando, no sé es importante ir apuntando ciertos puntos, etcétera……..

Resalta el señor Brenes Castillo: a mí me parece que la idea de don Alexander (Mejías) va en la línea de adelantar posibles consultas, para poder abordarlas desde un punto de vista técnico, pero no influye el no tener la discusión acá. Aunado a eso la moción iría en dos vías, posponer la discusión para la siguiente sesión, y no sé incitar a los miembros de Junta Directiva que así lo tuvieran a bien brindar las preguntas a más tardar el martes y con eso la Administración pueda saber la discusión, si les parece…..

Resalta la señora Arce Láscarez: tal vez yo le pondría un punto antes, que sería dar por recibido el informe de don Eddy (Martínez)……

Externa don Lizandro Brenes: no, es que el acuerdo de dar por recibido se dará una vez que tengamos la discusión……..

Pregunta doña Rita Arce: ¿por qué ahorita vamos a tomar acuerdo?.....

Indica el señor Brenes Castillo que: sería para posponer la discusión, y para remitir las consultas, igual la documentación ya la tenemos. Entonces muy bien, quienes estén a favor de esa propuesta sírvanse levantar la mano, okay, quienes estén de acuerdo en darle la firmeza al acuerdo sírvanse levantar la

mano, entonces queda aprobado de manera unánime y en firme con 7 votos de los que estamos aquí presentes…….

SE ACUERDA: de manera unánime y afirmativa, con siete votos presentes…….

5.a. Posponer la discusión de este punto para una próxima sesión…….

5.b. Instruir a los Directores para que remitan sus consultas al respecto sobre el ciberataque, a más tardar el próximo martes…….

CAPITULO IV		***OTROS ASUNTOS.***

ARTÍCULO 6.- ASUNTOS VARIOS.

6.a. Resalta doña Rosario Espinoza: yo quería presentar una moción con respecto a la sesión que tenemos para el lunes, dado que estamos asistiendo a las sesiones presenciales, el horario que pactamos principalmente por eso creo que los siete no estábamos conscientes de que los horarios que pusimos eran presenciales, los pusimos pensando en la virtualidad, y la sesión del lunes a las 6 de la mañana es físicamente imposible para muchos de nosotros venir, no solo venir, sino atender responsabilidades posteriores, porque podemos venir, el problema es por ejemplo; don Alexander (Mejías) que tiene que entrar a trabajar a las 7 de la mañana, igual yo y ustedes, entonces yo quisiera posponer la sesión de lunes, y en una próxima sesión de Junta poder discutir los horarios consecuentes tomando en cuenta la presencialidad……..

Externa don Lizandro Brenes: en discusión la moción; quienes estén a favor de esta propuesta sírvanse por favor levantar la mano; bajen la mano; quienes estén a favor de darle firmeza a esa propuesta sírvanse levantar la mano; queda aprobado con 7 votos y en firme de los que estamos aquí presentes….

SE ACUERDA: de manera unánime y afirmativa, con siete votos presentes…….

6.a.1. Posponer la sesión del próximo lunes 28 de noviembre 2022…….

6.b. Comenta doña Rita Arce: nada más tengo una observación para la compañera, y es que somos conscientes que viven en San José, las presas y todo esto, sin embargo, yo quisiera decirles que, si

quisiéramos sesionar en algún momento en el Colegio de Ingenieros, como para que no vengan hasta acá, yo estaría dispuesta a tratar de que vayamos ahí (…)…… Comenta don Juan Antonio Solano que: sí es factible realizar sesiones en otros sitios, nada más habría que tomar el acuerdo, que por ejemplo que digamos que la siguiente sesión es en el Colegio Federado, entonces se toma el acuerdo de hacer la sesión en tal lugar a tal hora, entonces sí es totalmente factible.. 6.c. Indica don Salvador Padilla: el proyecto N° 23.330 que es la reforma a la regla fiscal, tengo información de que se envió a la Junta Directiva la consulta, no sé si ya eso se tramito, ósea si ya se le está dando respuesta, nosotros ya habíamos solicitado el criterio que yo sé que lo estaban analizando en el departamento financiero, lo que quiero saber es si ya se le está dando trámite, contemplando el plazo reglamentario que son de 8 días hábiles para responder, sino se tendría que responder que se solicité una extensión…… Externa don Francisco Calvo: cuando la Asamblea (Legislativa) remite a JASEC proyectos de ley para consulta normalmente entra por 2 vías, o entra al correo de Georgina (Castillo) dirigiéndose en este caso al jerarca que es la Junta Directiva, o a veces llega a la Gerencia General por alguna razón, pero por lo general se refiere a la Junta Directiva, entonces por lo menos a la Gerencia no recuerdo, me parece que no, no sé Georgina (Castillo) si a la Junta Directiva ha llegado algo…….. Indica doña Georgina Castillo: eso es lo que estoy revisando en este momento, ya les digo…….. Externa don Juan Antonio Solano: sí, ya entró y el plazo vence mañana, está en análisis por el Área Financiera, porque no sólo es el artículo de la regla fiscal, sino que hay otros temitas fiscales, entonces el Área Financiera lo está viendo…….. Comenta el señor Padilla Villanueva: yo creo que sería bueno que pidieran una ampliación de plazo, que por tales razones la institución requiere un poco más de tiempo para que se muestre el interés sobre el tema, y que se va a responder en algún momento, esa es una recomendación. El otro es que vi otro proyecto muy interesante, está en la Asamblea Legislativa en la Comisión de Agropecuarios, que inclusive ya está en el plenario legislativo, es decir, ya salió de la Comisión de Agropecuarios y se están

conociendo mociones vía artículo N° 137, y este me parece muy importante, se titula así “Expediente 22.701 Reformas a la Ley Marco de Concesión para el Aprovechamiento de las Fuerzas Hidráulicas y a la Ley de Participación de las Cooperativas de Electrificación Rural y Empresas de Servicios Públicos Municipales en el Desarrollo Nacional”, echándole un ojo, obviamente hay que pedir el criterio de la parte técnica de JASEC, pero me parece que es un proyecto interesante, porque va en la línea de algo de una, a ver cómo decirlo sin que suene alarmista, es decir, hay una serie de proyectos ahorita actualmente en la Asamblea Legislativa, creo que ya llevamos como 7 criterios, yo a don Juan Antonio (Solano) le pasó dando trabajo a través de acuerdos, pero todo sea por el bien de la institución que pretenden una apertura mayor del mercado eléctrico, es decir, no una apertura descontrolada, ni una privatización total sino que más bien van en la línea de aperturar un poco el mercado eléctrico, dándole herramientas tanto a cooperativas, empresas de servicios públicos municipales que yo interpretaría que aquí entra también JASEC y la Empresa de Servicios Públicos de Heredia (ESPH), porque se ha pronunciado a favor del proyecto, está última y van muy avanzados en la corriente legislativa, el Gobierno ha tenido interés en ellos y varias fracciones han tenido interés, porque se parte del hecho que está apertura puede ser positiva para los usuarios en cuanto a los precios y tarifas, y entonces yo creo que con esta apertura que me parece que no es descabellada haciendo un mapeo amplio de los proyectos de ley, algunos piensan que es para beneficiar a cooperativas privadas o a sectores privados, o a generadores privados, y no están así porque JASEC en ese marco se ve beneficiado, siempre que está bien se le autoriza a un privado un poco más de libertades para la generación, o para la compra o para la generación y exportación de energía, o para la importación energía, pero cuando se hace eso también se está habilitando a empresas como JASEC, y eso puede resultar una oportunidad por ejemplo; cuando hablábamos de otro proyecto de ley que hablaba de que no solo el ICE pueda vender al mercado eléctrico regional, sino que JASEC puede hacerlo, y nosotros somos una institución pública, quienes se oponen al proyecto dicen que no que es para privatizar el ICE o para quebrarlo, o para desgraciarlo, y no, lo que no se dan cuenta es de que hay empresas estatales que siguen el interés público, pero la

idea de esto es pedir el criterio de este expediente que es el 22.701, osea que tomemos el acuerdo de pedirlo para la Asesoría Jurídica y de quien dependa la colaboración de ello, que tiene que ver con la generación hidráulica, y dar más posibilidades a empresas estatales como JASEC de que tengamos información y podamos pronunciarnos, y que lo conozcamos, entonces esa sería la propuesta, para que nos pronunciemos institucionalmente a favor o en contra, o haciendo posibles recomendaciones de mejora del expediente 22.701 que se tramita en la Asamblea Legislativa, su nombre es un poco largo y pomposo "Reformas a la Ley Marco de Concesión para el Aprovechamiento de las Fuerzas Hidráulicas y a Ley de Participación de las Cooperativas de Electrificación rural y Empresas de Servicios Públicos Municipales en el Desarrollo Nacional"……

Somete la Presidencia a votación la propuesta de don Salvador (Padilla)…….

Interviene don Alexander Mejías para indicar: yo quería decir algo con respecto a eso, que también que se de algún tipo de seguimiento, para que, en una razón del tiempo, como a futuro se den unos 15 o 20 minutos. lo que sea para empezar a dar seguimiento, para ver cómo va evolucionando y que no se nos quede ahí, ir mapeándolo para ver que va sucediendo…….

Resalta el señor Padilla Villanueva que: sería de mucha utilidad que nosotros pudiéramos ver eso, e incidir más en eso porque yo creo que tiene afectaciones a JASEC potentes digamos……...

Externa don Lizandro Brenes: muy bien en votación, quienes estén a favor sírvanse en levantar la mano; 6 votos porque yo no estoy votando a favor; quienes estén en contra; y abstenciones; y justifico mi voto, ese proyecto de ley no lo conozco, no conozco el contenido, probablemente ni siquiera está en el radar de la Cámara de Industrias de Costa Rica donde emiten posición, sin embargo, revisé la lista rápido y no aparece en la lista por eso es que no lo estoy votando pero prefiero abstenerme; entonces aun así queda aprobado con 6 votos a favor, bueno vamos a votar la firmeza; votemos la firmeza; en contra de la firmeza; y abstenciones; por ambas razones queda aprobado con 6 votos y en firme con 6 votos también, y una abstención del Director Brenes Castillo…….....

……..

SE ACUERDA: de manera unánime y en firme con seis votos presentes, y la abstención del director Brenes Castillo……..

6.c.1. Instruir a la Administración para que se pronuncie de manera institucional a favor o en contra, o haciendo posibles recomendaciones de mejora al expediente N° 22.701 "Reformas a la Ley Marco de Concesión para el Aprovechamiento de las Fuerzas Hidráulicas y a Ley de Participación de las Cooperativas de Electrificación rural y Empresas de Servicios Públicos Municipales en el Desarrollo Nacional"……..

6.d. Externa doña Rita Arce que: sobre el proyecto N° 23.471, hoy se aprobó en el plenario legislativo una moción de conformidad, este es de la Ley de Contratación Pública, de la entrada en vigencia, quizás más como para que lo mapeen y lo tengamos ahí, porque ese también nos afecta directamente, eso salió publicado……

Comenta don Lizandro Brenes que: a opinión personal, si usted me lo permite, bastante conveniente que esto se trámite de manera expedita y que se retrase un poquito más la entrada en vigencia de esa ley……

Resalta don Salvador Padilla que: me parece que ese proyecto está al borde de aprobarse, y efectivamente van a aprobar, porque si hay una disposición mayoritaria como se está notando de la Asamblea (Legislativa), y el Gobierno convocó quiere decir que están alineando los intereses y es muy probable que se apruebe, ahora sí hay que ver si lo logran publicar en la Gaceta antes de diciembre y toda la cuestión, o posterior, yo no sé cómo van a hacer, pero la cosa es que lo quieren aprobar nada más que están contra tiempo, verdad, pero es muy probable que sí se le extienda el plazo, pero hay que esperar, todo puede cambiar verdad, pero me parece que (…) como lo hablábamos en la sesión pasada que también tiene afectaciones para JASEC……

Resalta don Lizandro Brenes que: por favor la Administración tome nota; yo ya cedi mi tiempo; entonces sin más asuntos que tratar levantamos la sesión al ser las 22 horas con 18 minutos. Muchas gracias para todos, buenas noches, que estén muy bien……..

AL SER LAS VEINTIDOS HORAS CON DIECIOCHO MINUTOS SE LEVANTA LA SESIÓN.

LIZANDRO PAULITO BRENES CASTILLO (FIRMA)
Firmado digitalmente por LIZANDRO PAULITO BRENES CASTILLO (FIRMA)
Fecha: 2023.09.26 11:26:23 -06'00'

Bach. LIZANDRO BRENES CASTILLO
PRESIDENTE

LIZANDRO PAULITO BRENES CASTILLO (FIRMA)
Firmado digitalmente por LIZANDRO PAULITO BRENES CASTILLO (FIRMA)
Fecha: 2023.09.26 11:26:44 -06'00'

Bach. LIZANDRO BRENES CASTILLO
VOTO ABSTENCIÓN Art. 6.c.1.

ALEXANDER GERARDO MEJIAS ZAMORA (FIRMA)
Firmado digitalmente por ALEXANDER GERARDO MEJIAS ZAMORA (FIRMA)
Fecha: 2023.10.09 22:00:46 -06'00'

ALEXANDER MEJÍAS ZAMORA
VOTO ABSTENCIÓN Art. 3.a., 3.b.

ROSARIO ANDREA ESPINOZA CARAZO (FIRMA)
Firmado digitalmente por ROSARIO ANDREA ESPINOZA CARAZO (FIRMA)
Fecha: 2023.10.04 14:20:55 -06'00'

ROSARIO ESPINOZA CARAZO
VOTO ABSTENCIÓN Art. 3.a., 3.b.

SALVADOR PADILLA VILLANUEVA (FIRMA)
Firmado digitalmente por SALVADOR PADILLA VILLANUEVA (FIRMA)
Fecha: 2023.12.04 12:50:19 -06'00'

SALVADOR PADILLA VILLANUEVA
VOTO ABSTENCIÓN Art. 3.a., 3.b.

ANELENA SABATER CASTRO (FIRMA)
Firmado digitalmente por ANELENA SABATER CASTRO (FIRMA)
Fecha: 2023.10.03 16:52:28 -06'00'

ANELENA SABATER CASTRO
VOTO ABSTENCIÓN Art. 3.a., 3.b.

ANA LIA SOLANO PACHECO (FIRMA)
Firmado digitalmente por ANA LIA SOLANO PACHECO (FIRMA)
Fecha: 2023.09.14 14:07:43 -06'00'

ANA LÍA SOLANO PACHECO
VOTO ABSTENCIÓN Art. 3.a., 3.b.

AUDITOR INTERNO

La Auditoría Interna en cumplimiento a la Ley General de Control Interno Nº 8292 artículo Nº 22, inciso e), Capítulo IV, hace constar que aquí termina el acta número 059-2022 que incluye 64 folios.