E-BOOK

Minergy Connect y la CIBERSEGURIDAD

Sociedad Nacional de
MINERIA PETROLEO
Y ENERGIA

MINERGY
CONNECT

www.minergyconnect.pe

E-BOOK

Minergy Connect y la CIBERSEGURIDAD

Sociedad Nacional de
MINERIA PETROLEO
Y ENERGIA

MINERGY
CONNECT

www.minergyconnect.pe

02

RESUMEN

Minergy Connect es la comunidad digital de la industria minero energetico más importante del Perú. En consecuencia, la innovación y nuevas tecnologías son nuestros temas preferidos para conversar y compartir con nuestra audiencia. En este caso, nuestro segundo Ebook resume los últimos cuatro artículos relacionados a un interesante y vigente tema: La Ciberseguridad. Para ello, desarrollamos entrevistas en profundidad a eminencias en la materia, empresas de categoría mundial como Internexa y Telefónica nos acompañaron en esta oportunidad... ¡Muchas gracias a ellos!

A continuación se presentan cuatro artículos desarrollados por Minergy Connect, que se han desprendido de dos entrevistas en produndidad desarrolladas por el mismo equipo. En primera instancia, conversamos con Juan Camilo Ruiz, Senior Product Manager en InterNexa, empresa partner de Minergy Connect.

Nuestra segunda entrevista, fue realizada a Eleven Path, particularmente, a su Gerente de Operaciones Karla Parra. Nuestra destacada invitada tiene más de 15 años de experiencia en materias de telecomunicaciones, por lo que sin duda, al igual que Juan Camilo, tienen mucho que compartirnos.

Los cuatro artículos relacionados a ciberseguridad que encontrarás en este Ebook son lo siguientes:

- InterNexa: La importancia de la Ciberseguridad
- Internexa: Tecnicismos y desafíos propios de la Ciberseguridad
- Partners en Ciberseguridad
- Ciberseguridad en la industria minero energética

¡Gracias por leernos!

CONTENIDO

04

01 | INTERNEXA: LA IMPORTANCIA DE LA CIBERSEGURIDAD

05

INTERNEXA: LA IMPORTANCIA DE LA CIBERSEGURIDAD

Indiscutiblemente, la ciberseguridad es un verdadero desafío para las personas, empresas e incluso una preocupación a nivel país. Según recientes estudios realizados por Canalys, empresa líder en el análisis del mercado de tecnología global, el mercado de la ciberseguridad creció cerca de un 6% el presente año (luego de incrementarse más de un 10% en 2019), alcanzando un valor de 43.100 millones de dólares

Las organizaciones conviven cada vez más con redes interconectadas, tanto para el almacenamiento de archivos y procesamiento de datos, como para la operación de procesos críticos. La creciente digitalización del sector concede múltiples beneficios, pero al menos un gran problema: una mayor vulnerabilidad ante ciberataques.

InterNexa, partner de Minergy Connect, es una empresa dedicada a las telecomunicaciones y tecnologías de la información con más de 20 años de experiencia. Se ha especializado en acompañar los procesos de transformación digital de sus clientes con una oferta en servicios de conectividad, nube, seguridad, servicios administrados y analítica. Con más de 840 clientes en toda la región, InterNexa ha sido un aliado en TI y telecomunicaciones de diversas empresas en el Perú, de sectores como el minero, energético y educativo. En el presente artículo, profundizaremos acerca de lo que es, concretamente la ciberseguridad, basándonos en la visión e importancia que InterNexa da a este desafío, a través de Juan Camilo Ruiz, Product Manager.

06

El contexto mundial post pandemia, generó diversos impactos en la economía y en la forma de desarrollar un sin fin de procesos. Uno de ellos, el medio donde se desarrollan las actividades laborales. Se observa una orientación al trabajo remoto y según los pronósticos, es una tendencia que seguirá presente y en aumento. Esto quiere decir que no es sólo un evento coyuntural, sino una tendencia que podría ser protagonista durante las próximas décadas. Pronósticos de Regus, por ejemplo, estiman que hacia 2030 la demanda de teletrabajo aumentará en un 30% a medida que la generación Z pase a formar parte de lleno de la población activa y, por otra parte, el 73% de los equipos tendrá teletrabajadores en sus filas para 2028.

Esta tendencia representa un importante desafío en materia de ciberseguridad. Al estar “n” trabajadores operando de manera remota, se generan “n” puntos de vulnerabilidad para eventuales ataques, que son necesarios de proteger y que antes se concentraban en un solo lugar. Este es el primer gran argumento para explicar la preocupación (y ocupación) de personas, empresas y países por la ciberseguridad.

Los ataques no se están centrando sólo en organizaciones, sino también a nivel individual, llegando así a todas las escalas y niveles. Un caso común son los ataques del tipo “Ransomware”, en los que, en términos simples, el hacker implanta un criptogusano, como el famoso WannaCry de 2018, que bloquea el acceso a información relevante a través de su encriptación. Luego, comienza un proceso extorsivo, exigiendo a la organización o persona afectada una suma de dinero a cambio de recuperar el acceso a la información. El problema evidente es que el ciberdelincuente seguirá repitiendo esta conducta hasta que se tomen medidas en materia de ciberseguridad, para así detectar, eliminar y prevenir la introducción de softwares maliciosos.

Distinto es el caso de ciberataques en los que los delincuentes obtienen información personal y claves de los clientes a través de ingeniería social, principalmente mensajes falsos. Además del posible daño económico que puede significar una vulneración al sistema, existe también un irremediable daño en la imagen. El ataque afecta inmediatamente la confianza que proyecta una gran empresa dentro de su competitiva industria. Recordemos que la información es un activo importante y las organizaciones deben demostrar que son capaces de mantenerla segura.

07

Por último, se suma todo lo relacionado a la constante digitalización de procesos impulsado en parte por el Internet de las Cosas (IoT). Redes TO aisladas pasan a conectarse a internet, exponiendo infinitos dispositivos, con variadas tecnologías y complejidades a la red global. Todo esto hace a los sistemas operativos en general mucho más vulnerables, con mayores puntos débiles que los ciberdelincuentes[6] buscan incansablemente.

Lo anterior es particularmente relevante en una industria como la mineroenergética. Rápidamente se están integrando a sus operaciones críticas, dispositivos interconectados propensos a ataques. No es difícil pensar en vulnerar un taladro de perforación, una caldera de fundición, un dron o cámaras de seguridad, o lo que sea, con la finalidad de entorpecer el normal funcionamiento de una industria donde detener la producción es muy costoso. En definitiva, ningún sector por muy extractivista, operativo o convencional que sea, está ajeno a ciberataques, dada la transformación digital que vivimos.

Juan Camilo Ruiz, se desenvuelve en el ecosistema de la ciberseguridad desde 2003, cuando inició como “Hacker Amigo”. Este particular rol se encarga de detectar puntos débiles o de vulnerabilidad en los sistemas con la finalidad de prevenirlos, representando la base de cualquier servicio de ciberseguridad: diagnóstico de la red y eventuales puntos propensos a ataques, para luego abordarlos de la manera más eficiente y menos costosa.

Esta formación proactiva en ciberseguridad sirvió, según Juan Camilo, para “ponerse en los zapatos del ciberdelincuente”, vale decir, anticiparse a su actuar. “Muchas veces, el hacker hace de estos ataques su trabajo, y al igual que todos, lo optimiza para obtener mayores ganancias al menor esfuerzo. Esto se debe considerar en la construcción de cualquier sistema de ciberseguridad”, sentencia el experto.

En los próximos artículos profundizaremos acerca de las tres capas que deben considerarse en un sistema de ciberseguridad, además de comprender la necesidad de un cambio estructural, mejora continua y la importancia de relacionarse con partners en materias de seguridad en red, y que, por cierto, basen su servicio según los requerimientos de cada cliente.

08

02 | INTERNEXA: TECNICISMOS Y DESAFÍOS PROPIOS DE LA CIBERSEGURIDAD

09

INTERNEXA: TECNICISMOS Y DESAFÍOS PROPIOS DE LA CIBERSEGURIDAD

En el presente documento, profundizaremos acerca de la ciberseguridad, basándonos en la visión e importancia de este desafío. Para ello, seguiremos conversando con Juan Camilo Ruiz, Senior Product Manager en InterNexa, empresa partner de Minergy Connect.

Para nuestro especialista, Juan Camilo Ruiz, la ciberseguridad corresponde a "Todos los mecanismos que se establecen para proteger el acceso a la información, entendiendo que dicha data tiene diferentes niveles de acceso dependiendo de cada usuario, y solo algunos de ellos están autorizados para modificarlos". La información presenta tres niveles o capas, y es importante para cualquier sistema de ciberseguridad comprender y operar sobre ellos. Estos son: la visualización, integridad y ubicación de los datos.

En términos concretos, es importante monitorear y gestionar la seguridad en estos tres niveles de la información. En primer lugar, que la visualización sea oportuna y confiable. No se trata que sea simplemente visible, sino que sea notoria por quien corresponda, entendiendo que, en toda organización, ciertos usuarios están facultados para visualizar cierto tipo de archivos. Una amenaza en este nivel, por ejemplo, es un ataque a un banco que haga públicas las cuentas de muchos de sus clientes. La información sigue ahí y no fue mal utilizada, simplemente se hizo pública, convirtiéndose en un hecho muy costoso para la entidad, en relación a su reputación.

Algo similar ocurre con los otros dos niveles. La integridad corresponde a la capacidad de modificar la información, mientras que la ubicación al lugar físico donde se almacena. La vulneración a cualquiera de estos niveles es perjudicial para la persona u organización víctima del atentado, por tanto, un sistema de ciberseguridad debe considerar resguardar estas tres aristas de los datos.

Al entender estos niveles podemos, de alguna manera, dimensionar la importancia de la ciberseguridad en el sentido que, como usuarios, somos continuamente vulnerables ante ciberataques. El hacker posee muchas herramientas o “frentes” para atacar y extorsionar, motivo por el cual la modalidad Ransomware se volvió protagonista. Los ataques tienen la particularidad de encriptar la información, imposibilitando su visualización y, por tanto, su uso, desvalorizando al 100% este importante activo. Esto explica la tendencia de vulnerar a cualquier blanco, incluso una persona natural, sin mucha información aparentemente a proteger. El hacker a través de ataques masivos, busca captar una decena de víctimas para bloquear su información y luego exigir permanentemente un pago para su liberación. Además, dentro de las amenazas encontramos al Phishing y los ataques Volumétricos.

En base a lo anterior, se explica la necesidad de invertir y controlar continuamente los sistemas de ciberseguridad, dado que los tipos de ataque están en constante evolución. La visión de InterNexa sobre la ciberseguridad es de 360º. Esto implica dos cosas fundamentalmente. En primer lugar, “entender que los sistemas y por tanto necesidades de cada cliente son distintas”. Es imposible pensar en un servicio de ciberseguridad que sea igual para todas las organizaciones, puesto que, por el simple hecho de tener una propuesta de valor distinta, tendrá otros intereses de seguridad. Presentará procesos diferentes, y, por tanto, puntos de vulnerabilidad totalmente diversos, sumado a que cada grupo humano no tiene la misma educación digital y tiene cierto grado de resistencia al cambio.

Esto provoca un segundo gran desafío reconocido por el experto, que radica en la necesidad de un control (y por tanto inversión) constante en materias de ciberseguridad. “La posibilidad de un ciberataque siempre está latente, esto porque el hacker busca continuamente nuevas superficies y vectores de ataque en los sistemas de la organización”. En definitiva, para Juan Camilo e InterNexa, la ciberseguridad debe ser 360°, las 24 horas del día y los 7 días de la semana. “Es un proceso de mejoramiento continuo”.

Por último, quisiéramos transmitir a toda la comunidad minero energética, la idea principal de Juan Camilo en nuestra entrevista. Esta radica en la necesidad de desmitificar la ciberseguridad. Actualmente se ve como un mito y evidentemente en base a todo lo expuesto, no lo es.

Comúnmente se piensa que solamente es una preocupación para grandes organizaciones, esto no es cierto. Ninguna compañía (e incluso persona) está ajena a ciberataques, dado que todos, producto de la pandemia y transformación digital, orientamos las actividades hacia una mayor interconexión. Lo que se necesita es entender la ciberseguridad como un proceso constante y es preciso disponer de un aliado como InterNexa, que entienda las necesidades y genere condiciones seguras para seguir vigentes como empresa.

03 | PARTNERS EN CIBERSEGURIDAD

PARTNERS EN CIBERSEGURIDAD

En este artículo nos enfocamos y pensamos en un nivel organizacional. Abordaremos el mercado de ciberseguridad en cuanto a sus proveedores, servicios, industria, tendencias y más. En base a lo anterior, entender el rol y visión de una empresa como Telefónica Tech en materia de ciberseguridad resulta muy útil.

Telefónica apuesta por acelerar los servicios digitales con mayor potencial de crecimiento, tales como ciberseguridad y cloud, mediante la creación de Telefónica Tech. El equipo de ciberseguridad de Telefónica Tech, conocido como ElevenPaths, está enfocado en la prevención, detección y respuesta adecuada para disminuir los ataques cibernéticos y proteger los servicios digitales a fin de garantizar la ciber-resiliencia dentro de la organización.

Karla Parra, Gerente de Operaciones de Telefónica Tech conversó con nosotros sobre ciberseguridad. Al igual que otros expertos, Karla precisa contextualizar acerca de cómo la conectividad y transformación digital, impulsada por la pandemia Covid-19, han acelerado la implementación de múltiples herramientas y tecnologías, ya que existe una mayor cantidad de puntos débiles que son necesarios proteger de diversas maneras, más aún trabajando en modo remoto. Es importante comprender la ciberseguridad como un desafío estructural y transversal que afecta todas las escalas de la organización. A modo de ejemplo, los ataques tipo Phishing buscan que la víctima entregue sus claves de acceso para vulnerar el sistema.

Telefónica apuesta por acelerar los servicios digitales con mayor potencial de crecimiento, tales como ciberseguridad y cloud, mediante la creación de Telefónica Tech. El equipo de ciberseguridad de Telefónica Tech, conocido como ElevenPaths, está enfocado en la prevención, detección y respuesta adecuada para disminuir los ataques cibernéticos y proteger los servicios digitales a fin de garantizar la ciber-resiliencia dentro de la organización.

Karla Parra, Gerente de Operaciones de Telefónica Tech conversó con nosotros sobre ciberseguridad. Al igual que otros expertos, Karla precisa contextualizar acerca de cómo la conectividad y transformación digital, impulsada por la pandemia Covid-19, han acelerado la implementación de múltiples herramientas y tecnologías, ya que existe una mayor cantidad de puntos débiles que son necesarios proteger de diversas maneras, más aún trabajando en modo remoto. Es importante comprender la ciberseguridad como un desafío estructural y transversal que afecta todas las escalas de la organización. A modo de ejemplo, los ataques tipo Phishing buscan que la víctima entregue sus claves de acceso para vulnerar el sistema.

El problema es que la responsabilidad acerca de un ciberataque es muy confusa. No se sabe con certeza si fue producto de una vulnerabilidad en el sistema o bien del usuario, quien entrega las claves producto de un engaño.

Sea como sea, determinar la responsabilidad ante un ciberataque se vuelve prácticamente imposible para el cliente, acompañado de un costoso proceso forense. Para evitarlo, muchos de los servicios ofrecidos por proveedores de ciberseguridad hoy en el mercado, incluyen seguros. En la industria bancaria, por ejemplo, esta modalidad de ataques Phishing es altamente frecuente y según la organización multinacional Sophos1, el 53% de los ataques están dirigidos, en mayor medida, al usuario o cliente final. El modus operandi consiste en engañar al operador haciéndole ver un espacio confiable y seguro para que éste entregue accesos de valor. Por tanto, para Karla es primordial educar al equipo acerca de los riesgos y exposiciones hacia el cibercrimen.

Al entender la necesidad de contar con un socio experto en ciberseguridad, encontramos a Telefónica Tech. Karla nos comenta que en la compañía “la idea es desafiar el estado actual de la seguridad, creemos que es posible un mundo digital más seguro. Apoyamos a nuestros clientes en su transformación digital, creando innovación disruptiva, aportando la privacidad y la confianza necesaria en nuestra vida digital diaria”. Cada cliente de Telefónica es distinto. Éstos tienen diferentes tamaños, procesos y giros y por ende tienen necesidades diferentes y precisan de un sistema de protección específico.

Asimismo, agrega que “tenemos como misión hacer que la seguridad sea más humana y generar confianza entre las personas, en un mundo donde las ciberamenazas son inevitables. Nosotros como proveedores de servicios de seguridad gestionada nos centramos en la prevención, detección y respuesta adecuada para reducir los ataques, proteger sus servicios digitales y así garantizar que su negocio sea ciber-resiliente, anticipándonos a los ataques más sofisticados y frecuentes”. En base a lo anterior, la necesidad de contar con un aliado en ciberseguridad radica en la creciente frecuencia y sofisticación de los ataques, pudiendo llegar a todos los servicios y niveles de la empresa. Es clave para un sistema de ciberseguridad ser proactivo y tener una cultura de mejoramiento continuo en los siguientes tres niveles:

Hoy en día, el desarrollo de productos y servicios para grandes empresas, sobre todo ligadas a la tecnología e información, están pensados para proteger la vulnerabilidad digital. Ya no es una preocupación eventual y pasajera para las organizaciones, sino una arista que es necesario considerar desde la gestación de un servicio, producto o proyecto; por ello se vuelve necesario contar con un equipo dedicado a la ciberseguridad que tenga como responsabilidad primordial el resguardo de información valiosa para la compañía. Se trata, por tanto, de una inversión permanente y un cambio estructural.

En cuanto al mercado y proveedores en materias de ciberseguridad encontramos algunos de los grandes jugadores de la industria tales como IBM, Deloitte, InterNexa y Telefónica con Telefónica Tech. Es necesario que el proveedor esté un paso adelante en relación a los hackers, por lo que tener equipos de trabajo proactivos se vuelve un factor crítico de éxito.

Para finalizar, quisiéramos invitarlos a seguir informándose sobre las bondades de la ciberseguridad. ElevenPaths dispone de un blog2 en su página web con contenido interesante acerca de nuevas tecnologías, tendencias, telecomunicaciones y ciberseguridad, tanto a nivel individual como organizacional. Invitamos a la comunidad a revisar el material disponible para la industria mineroenergética.

1. Artículo “The Impossible Puzzle of Cybersecurity”
2. https://empresas.blogthinkbig.com/elevenpaths/

04| CIBERSEGURIDAD EN LA INDUSTRIA MINEROENERGÉTICA

CIBERSEGURIDAD EN LA INDUSTRIA MINEROENERGÉTICA

La pandemia, la transformación digital, la modernización de los procesos y la industria 4.0 han implicado múltiples beneficios y desafíos. Uno evidente es la ciberseguridad debido a la creciente frecuencia y diversidad de los ataques. En los artículos anteriores sobre este importante tema ha quedado en evidencia la capacidad de estos ataques para afectar a cualquier tipo de organización y en cualquier nivel de la misma. ¿Ocurre lo mismo en nuestra industria minero energética?

Durante nuestros últimos artículos, ha quedado en evidencia la necesidad de abordar el desafío de la ciberseguridad de manera holística y estructural. Producto de la transformación digital y el contexto de pandemia actual, se han incrementado los ciberataques en cuanto a su frecuencia y dinamismo, lo cual ha aumentado también los niveles de inversión destinados a este servicio. Estudios estiman que alrededor de 6,000 millones de dólares se perderán globalmente derivado de la actividad cibercriminal durante el 2021. Ahora bien, ¿ocurre lo mismo en Perú? ¿qué pasa con la industria minero energética? Karla Parra, gerente de Operaciones de Telefónica Tech, nos ayuda a entender de mejor manera los riesgos a los cuales están expuestas las empresas del sector.

Según estudios de EY Building a better working world[1], el 51% de las compañías en el Perú sostienen que la relación entre ciberseguridad y sus líneas de negocio es inexistente o neutral. Asimismo, determina que tan solo el 27% de las compañías en el Perú incluyen la ciberseguridad en la planificación de nuevas iniciativas. En definitiva, se reconoce como una necesidad y riesgo inminente, pero aún no se toman las medidas necesarias, quedando totalmente vulnerables a ataques de este estilo.

Es evidente que la industria minero energética no es ajena a ciberataques y pensar lo contrario podría significar un grave error. En general, la industria minero energética se caracteriza por ser conservadora y tradicional en cuanto a la aplicación de nuevas herramientas. En la práctica, muchas compañías mineras están actuando cuando ya es demasiado tarde para gestionar los riesgos y vulnerabilidades en sus sistemas. Esto expone innecesariamente a la empresa a mayores y variadas amenazas.

La responsabilidad de gestionar la exposición a los riesgos de ciberataques no se puede delegar en una o dos personas, sino que debe reunirse un amplio equipo de responsables para formar una visión única, coherente y accesible al entorno de amenazas cibernéticas.

Según la encuesta “Global Information Securiry Survey 2017” realizada por EY, se estima que un 53% de las empresas de energía y recursos naturales ha incrementado su gasto en ciberseguridad en los últimos 12 meses. Sumado a un contexto de pandemia, es evidente que los presupuestos destinados a esta área están al alza, pero no lo suficiente como para solventar los riesgos de manera efectiva, particularmente con respecto al crecimiento de amenazas en Redes/Tecnologías Operacionales (TO), producto de la irrupción del IoT y su apertura al internet.

Aquí es necesario detenerse, ya que para entender la relación y preocupación entre los ciberataques y la industria minero energética, se debe entender también la distinción y creciente conexión entre Tecnologías de la Información (TI), Tecnologías de la Operación (TO) y Seguridad Física (SF). Hasta ahora, los mundos de TI, TO y SF han sido tradicionalmente independientes, situación que actualmente ha cambiado dado que las necesidades de los entornos están cada vez más ligados, haciéndose parte incluso de un mismo proceso. Por su parte, indiscutiblemente la industria es intensiva en el uso de TO (maquinarias, excavadoras, termómetros, sofisticados medidores, recientemente drones, etc.) así como de SF (sistemas de control de accesos digitales, cámaras IP, entre otros) pero también está incorporándose TI en la ejecución de prácticamente todos sus procesos.

El incremento de conectividad de los sistemas industriales y la integración de las tecnologías con otras contribuye a incrementar las amenazas, según Parra. Algo normal para las compañías de energía y minería es la creciente dependencia en sistemas de automatización, centros de operaciones remotas y toma de decisiones en tiempo real. Si bien lo anterior genera una mayor eficiencia, ofrece también una mayor vulnerabilidad para eventuales ciberataques.

La ciberseguridad debe verse a nivel holístico, donde la clave está en la correcta gestión de la misma (prevenir, detectar, dar respuesta) garantizando la ciber-resiliencia, buscando proteger la confidencialidad, integridad y disponibilidad de la información de los sistemas en su entorno.

En la actualidad, se han identificado cuatro puntos o "Rutas de Ataque" que deben proteger las organizaciones de la industria:

1. Los sistemas y redes (redes planas, protocolos inseguros, software antiguos y desactualizados)
2. Accesos remotos inseguros
3. Malware (USB o email)
4. Ingeniería Social

Por su parte, los hackers vulneran estas rutas utilizando patrones en los puntos débiles dentro de la arquitectura de la red, tecnologías heredadas, personal remoto, accesos de terceros (cuyo descontrol se ha incrementado dada la pandemia) por lo que se vuelve necesario contar con partners en materias de ciberseguridad que entreguen un servicio específico a cada industria y cliente. Ante este panorama las empresas minero energéticas deben adoptar un marco de ciberseguridad para la identificación de fallas en las "rutas" clave de sus procesos de negocio, aparición de nuevas amenazas y acciones necesarias para mantener a la organización y a sus trabajadores fuera de peligro. Independientemente del marco que se adopte, se debe contar con un enfoque basado en riesgo, que mantenga un equilibrio entre "proteger" y "reaccionar", y que cumpla con las necesidades operacionales de la compañía.

[1] https://www.ey.com/es_pe/news/2020/06/ciberseguridad-lineas-negocio-neutral
[2] https://www.incibe-cert.es/