ESTRATEGIAS DE SEGURIDAD EN ESQUEMAS DE TRABAJO REMOTO

Resumen

Al momento de implementar esquemas de trabajo remoto, debes tener en cuenta las posibles aristas que comprenden la infraestructura tecnológica de tu organización y que permiten el correcto funcionamiento de plataformas como correo electrónico, VPN (Virtual Private Network), equipos de usuario final, entre otros, ya que son estas las que permiten la operación diaria en la empresa. Es por este motivo, que debes asegurar la información y los diferentes componentes tecnológicos que la soportan, buscando evitar impactos reputacionales, regulatorios, operativos, financieros y demás, que se pueden generar como consecuencia de un ataque informático. Para esto, te presentamos algunos escenarios que pueden poner en riesgo a tu empresa cuando se usan esquemas de trabajo remoto, además de recomendaciones útiles en la labor de protegerlas.

Protección al empleado en trabajo remoto

La información es, sin duda alguna, el ADN de las empresas. Es el motor que permite gestar relaciones y se constituye en un insumo relevante para la definición de los objetivos estratégicos de las organizaciones, es por esto por lo que se debe resguardar con tanto esmero. Una protección que debe estar fundamentada en los actores más relevantes para la gestión de tu empresa: las personas, la tecnología y los procesos. En este sentido, te compartimos varias recomendaciones referentes a salvaguardar la información que reposa en los equipos tecnológicos de los empleados en esquemas de trabajo remoto.

1

Para robustecer las estaciones de trabajo o endpoints, tan codiciadas en los esquemas de trabajo remoto por los ciberdelincuentes, puedes apoyarte de soluciones antimalware o Endpoint Detection and Response (EDR), desplegadas en los equipos de la compañía, de tal forma que ante una descarga de software malicioso derivada de la recepción de un correo electrónico o la visita a un sitio web, se pueda proteger la información para evitar que sea robada, el secuestro del equipo y demás riesgos posibles. Procura habilitar la opción en el antimalware que permita únicamente la ejecución del software empresarial, evitando así la ejecución de cualquier otro programa instalado, esto te protegerá de programas indeseados. Bajo estas condiciones, recomendamos mantener actualizado este sistema para salvaguardar a los empleados frente a las amenazas más recientes en el mundo digital.

2

Para evitar que los colaboradores naveguen en páginas riesgosas que puedan robar su información o descargar código malicioso en sus equipos, sugerimos contar con un sistema de control de navegación, bien sea potenciado desde el sistema antimalware o uno específico para esta labor, de tal forma que, si el empleado da clic sobre un enlace malicioso al navegar en su equipo corporativo, no lo lleve al sitio amenazado y prevenga el acceso a su información por parte de cibercriminales.

3

Proteger los sistemas de correo electrónico es fundamental para las empresas ya que es por allí, por donde ingresan la mayoría de los ataques hacia los empleados. Para esto, se podrán habilitar sistemas de tipo antispam que serán fundamentales para evitar la llegada de correos maliciosos (también llamados phishing). Además, debes contar con protecciones como sandboxing, que permitan detectar adjuntos maliciosos enviados por ciberdelincuentes en los correos, de tal forma que eviten que estos lleguen a los colaboradores y les pueda representar algún daño sobre sus máquinas o información. De manera similar, para el envío de correos por parte de la compañía, es relevante contar con protecciones de tipo Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) y Domain-based Message Authentication, Reporting, and Conformance (DMARC), de tal forma que, a nivel técnico, se pueda hacer frente a correos amenazantes que intenten suplantar a la empresa.

4

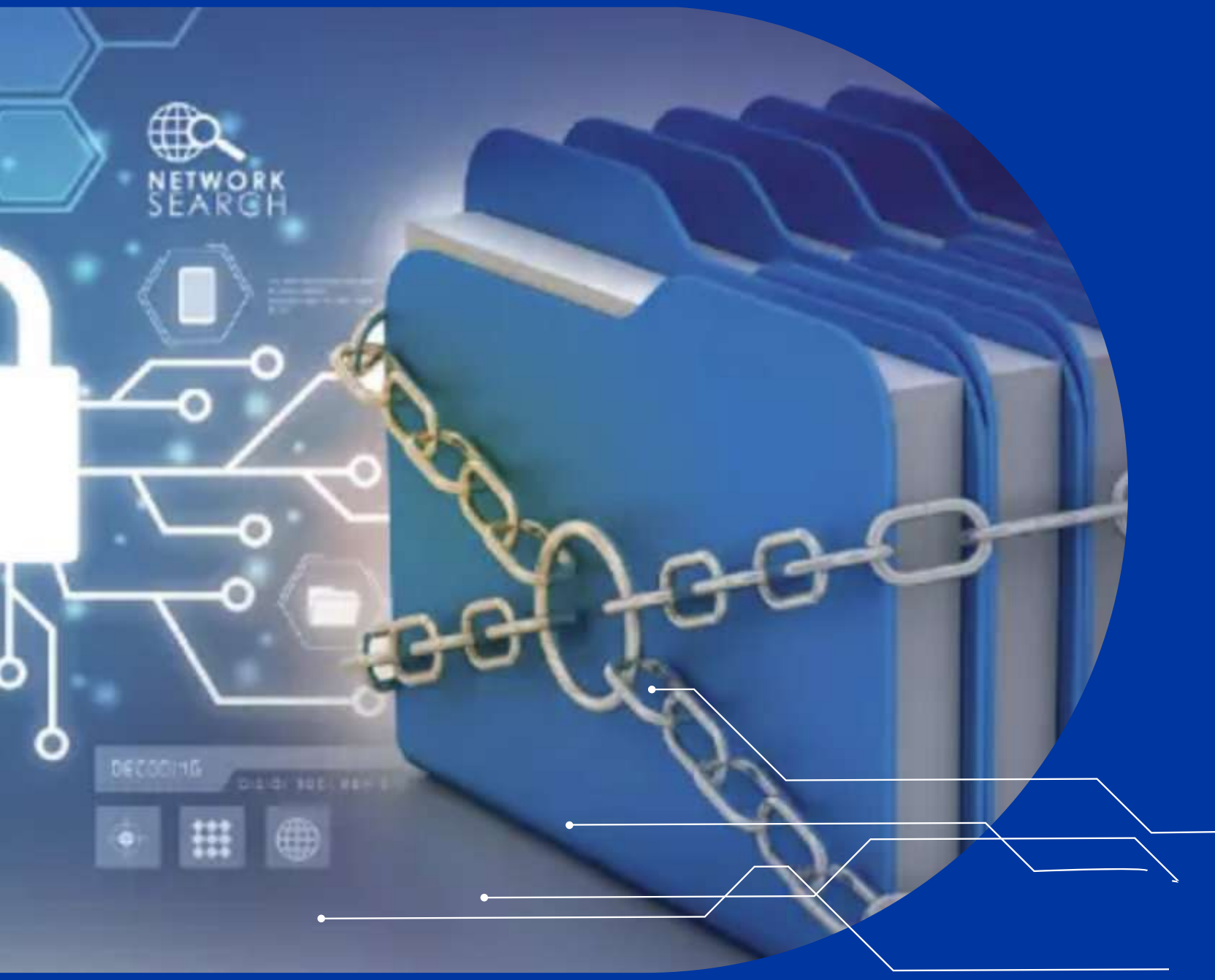
Para evitar que ciberdelincuentes puedan suplantar técnicamente el dominio de correo de la empresa y con esto puedan enviar correos maliciosos o phishing a los empleados, podremos configurar políticas Sender Policy Framework (SPF), incluyendo explícitamente los dominios, IP o rangos de IP autorizados para enviar correo a nombre de la empresa seguidos por -all, de manera que sea lo más concreta y restrictiva posible, limitando así las acciones que los ciberdelincuentes puedan realizar sobre dichos dominios.

5

Frente al uso de herramientas colaborativas y de comunicación como Teams, Zoom, Webex, entre otras, es importante habilitar el segundo factor de autenticación, así como la opción de una sala de espera para admitir o denegar el acceso de invitados y evitar huéspedes indeseados que puedan irrumpir en reuniones corporativas. Será igual de importante mantener estos sistemas actualizados para impedir la intrusión de un cibercriminal por brechas de seguridad en versiones anteriores.

6

Poder tener una gestión remota sobre la distribución de software y parches de seguridad a los equipos de la compañía que operen en trabajo remoto, será crucial para controlar la obsolescencia del software y evitar materialización del riesgo, debido a posibles brechas de seguridad que estas versiones obsoletas puedan tener.



7

Para evitar que un atacante pueda obtener información relevante sobre la empresa y sus empleados en equipos corporativos robados físicamente es fundamental utilizar cifrado de disco que asegure la información en reposo y complique la labor del atacante para obtenerla.

Recomendaciones de seguridad para el acceso a red interna en modalidad de trabajo remoto

En las diversas modalidades de trabajo remoto es frecuente tener la necesidad de acceso a las aplicaciones propias de la compañía por parte de los colaboradores que se encuentran en casa, para que puedan trabajar como si estuvieran en sitio. Para habilitar el acceso a estos sistemas hay diversos retos tecnológicos y de seguridad que se deben sortear para evitar exponer más información e infraestructura de la estrictamente requeridas que pueden ser utilizadas por cibercriminales para atacar la compañía.

1

Una recomendación para dar acceso a los empleados a redes internas de forma segura será la implementación o potenciación de una solución VPN (Virtual Private Network), que evite publicar a Internet servicios internos, pero que permita que aquellos empleados con la debida autorización puedan entrar a la red corporativa. **De esta forma se reduce la superficie de ataque.**

2

El uso de internet por parte de los colaboradores en modalidad de trabajo remoto no será siempre dirigido hacia las aplicaciones internas de la compañía, sino también hacia servicios externos de terceros como por ejemplo Google, Bing, servicios en la nube, entre otros, y es por esto por lo que cuando estén conectados a la solución VPN de la empresa deberás optimizar el ancho de banda en tu compañía para no saturar la red y permitir su disponibilidad. Para ello, podrás hacer uso del modo split que posibilitan las soluciones VPN, permitiendo enrutar únicamente hacia la intranet, el tráfico correspondiente a las aplicaciones en sitio y el consumo restante generado, hacia plataformas que se encuentren en internet, canalizándolo por la IP pública de los colaboradores, de modo que se logre reducir el consumo de ancho de banda de la empresa. Es importante considerar que al evitar que este tráfico externo circule por la red interna de la compañía, no se podrá proteger al usuario como generalmente se hacía, restringiendo la navegación a páginas maliciosas desde el firewall interno, se deberán implementar salvaguardas en las estaciones de usuario final que se encarguen de estas medidas al hacer uso, por ejemplo, de controles de navegación apalancados por soluciones enfocadas a este fin o incluso por medio de plataformas antimalware que tengan algún módulo de control de navegación. Así, cuando el usuario navega a un enlace malicioso, el control de navegación podrá protegerlo.

3

En las modalidades de trabajo remoto es frecuente que ciberdelincuentes intenten acceder a la infraestructura interna de la empresa a través, por ejemplo, de accesos VPN de los empleados. Robustecer por medio de la implementación de un segundo factor de autenticación en el ingreso, dificultará la labor del ciberdelincuente al intentar ingresar a la red interna, ya que además de conocer las credenciales del usuario, deberá conocer una segunda clave o factor y de esta forma se protegen los accesos.

4

Para permitir que los usuarios sigan teniendo los mismos accesos a sus aplicaciones, tanto en sitio como en trabajo remoto y evitar que ganen o pierdan privilegios indeseados, **podrás integrar el acceso VPN con el directorio activo de la compañía,** de tal forma que sea este último el que continúe dando los accesos a las aplicaciones de manera centralizada y se protejan así los sistemas e información.

Protección de aplicaciones

Al momento de facilitar el acceso y flexibilizar la movilidad para los empleados en esquemas de trabajo remoto, se debe pensar también en fortalecer la seguridad de la infraestructura tecnológica en una red interna, pues será esta la que en últimas deberá soportar la carga de los usuarios.

1

La segregación de accesos y operaciones en las aplicaciones es importante para mitigar el éxito de ciberataques desde el interior y exterior de la empresa, **ya que permite entregar a cada empleado únicamente los permisos necesarios para ejecutar sus labores, basados en el mínimo privilegio posible.** A su vez, permite tener una jerarquía organizada requerida para la implementación de estándares como ISO 27001, PCI DSS, HIPAA, SOX, entre otros.

2

Centralizar los sistemas de autenticación y autorización de la compañía, permite gestionarlos de una manera **óptima y focalizar los esfuerzos en asegurar dicho punto de entrada.**

3

Es importante tener en cuenta que en los casos en los cuales se deben exponer algunas aplicaciones o sitios web a internet, para efectos por ejemplo de relacionamiento con los clientes, **es posible fortalecer la seguridad de las páginas web por medio de la habilitación de HyperText Transfer Protocol Secure (HTTPS), con suites de cifrado seguras como Transport Layer Security (TLS) 1.2 y 1.3**; deshabilitando por ejemplo, suites de cifrado como TLS 1.0 y 1.1, Secure Socket Layer (SSL) 3.0 en modo Cipher-Block Chaining (CBC), entre otras, de tal forma que se proteja la información en tránsito. Igualmente, configurar HTTP Strict Transport Security (HSTS) en las plataformas, permite tener una mayor protección frente a ataques como Hombre en el Medio o Man in The Middle (MiTM) enfocados en robar la información en movimiento.

4

Como no todas las personas que acceden a los sitios web corporativos lo hacen con buena intención, **debes implementar protecciones como Web Application Firewall (WAF), que nos permite protegernos frente a ataques comunes como Cross-Site-Scripting (XSS), Inyección SQL (SQLi), ataques de fuerza bruta o incluso Denegación de Servicios (DoS, DDoS), salvaguardando de esta forma la información hospedada en dichas páginas.** También será muy importante poder habilitar la trazabilidad sobre las funcionalidades críticas de estas aplicaciones como, por ejemplo, el login o autenticación (ingreso de usuario y contraseña) o alguna opción transaccional relevante, recopilando la dirección IP, hora de ejecución y demás, con el fin de poder hacer seguimiento a usuarios malintencionados y tomar acciones al respecto.

5

Las vulnerabilidades existentes en plataformas tecnológicas utilizadas por las empresas conllevan a la **materialización de riesgos cibernéticos que generan impactos desde lo financiero, reputacional o legal,** los cuales pueden causar pérdidas que podrían ascender al rededor de los 2.000 SMMLV (Salarios Mínimos Mensuales Legales Vigentes) derivados de un incumplimiento a la Ley de Protección de Datos Personales (Ley 1581 de 2012). Por esto, realizar pruebas de seguridad sobre estos activos digitales es tan importante para identificar, analizar y valorar las vulnerabilidades encontradas y así poderlas gestionar a tiempo antes de que generen una materialización.

6

Cada vez más los ciberdelincuentes encuentran maneras de vulnerar los sistemas y saltar protecciones habilitadas en las aplicaciones. Por eso deberás fortalecer los sistemas de protección a nivel de red, como el firewall, el Sistema de Detección de Intrusos (IDS), el Sistema de Prevención de Intrusos (IPS), el Web Application Firewall (WAF), de tal forma que se pueda tener mayor capacidad de detección, contención y reacción ante un ataque cibernético. Si los sistemas utilizados están basados en firmas de detección de amenazas, valida cada cuánto se actualizan y si el proceso es manual o automático, y establece validaciones periódicas de actualización que habiliten la protección frente a las amenazas más recientes.

Ciber resiliencia o capacidad de recuperarse de forma rápida ante un ciberataque

Existen diversos tipos de ataques cibernéticos que pueden generar interrupciones en el negocio, indisponibilidad de las plataformas tecnológicas, entre otras. Es en estos casos, en los cuales, para mitigar el impacto, se deberá implantar la cultura del backup o de resguardo, que nos permita responder frente a un evento de contingencia y garantizar la continuidad del negocio.

1

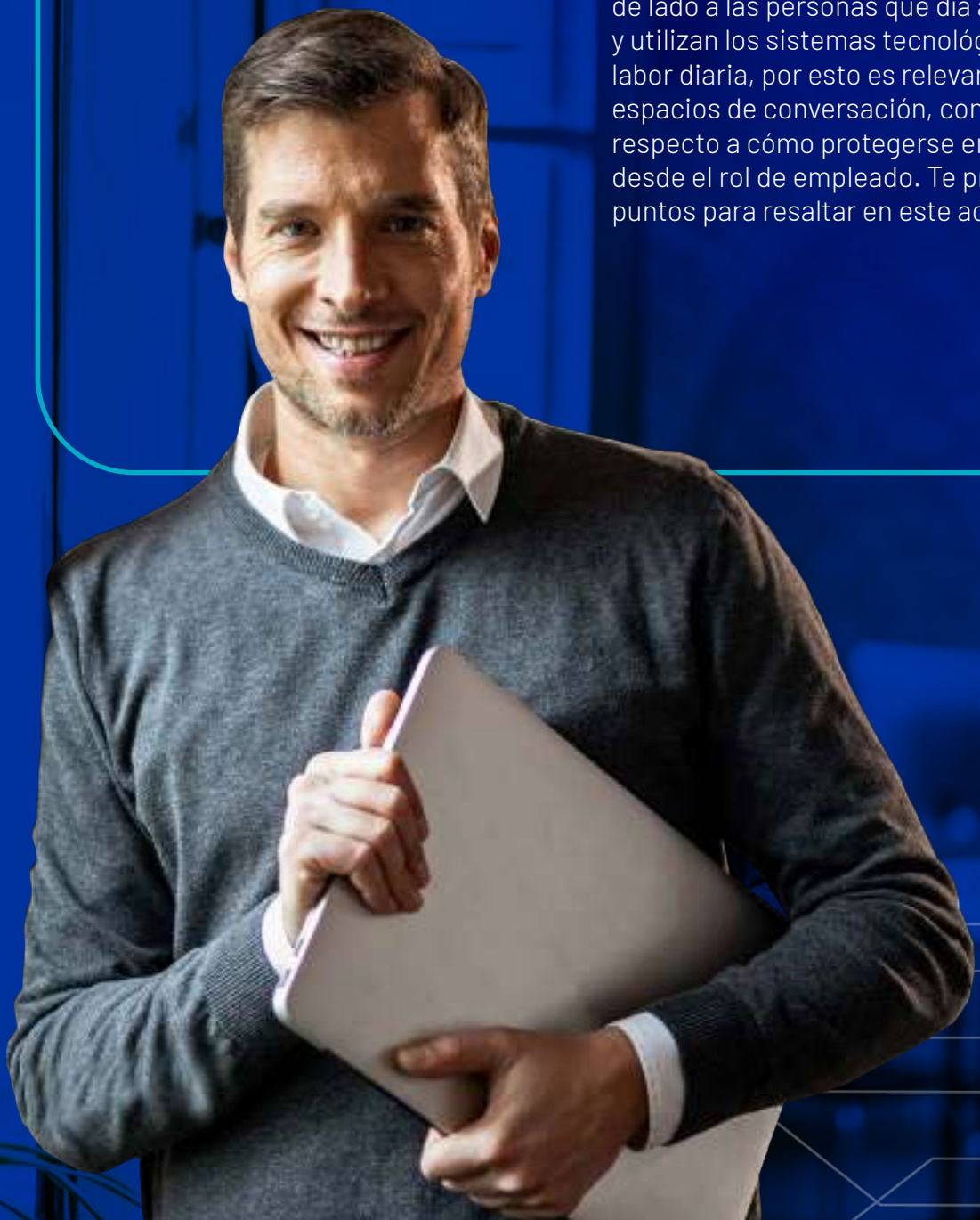
En búsqueda de optimizar tu presupuesto deberás ser muy selectivo en las apuestas que se toman en pro de la seguridad de la compañía. Establecer cuáles son las aplicaciones y bases de datos críticas BIA (Business Impact Analysis) para el negocio, será fundamental para focalizar los esfuerzos de seguridad sobre dichos activos y proteger la información que en ellos reposa, para ser eficientes y efectivos en la protección.

2

Para que los usuarios puedan ingresar a los sistemas con los que día a día laboran, será muy importante que garantices un nivel de conexión adecuado. Para ello deberás realizar un dimensionamiento apropiado de los recursos de red, la capacidad de cómputo y almacenamiento, que puedan soportar la carga de conexiones, incrementadas en los consumos hacia los servidores debido al trabajo remoto. Realizar un monitoreo constante sobre dichos consumos, te permitirá identificar el momento oportuno en que debas escalar la infraestructura y dar continuidad al negocio.

Cultura de ciberseguridad para los empleados

En definitiva, el trabajo remoto trae unos retos importantes que deben abordarse de la mano de la seguridad, para que la continuidad del negocio pueda seguir siendo una realidad. Igualmente, no se debe dejar de lado a las personas que día a día construyen empresa y utilizan los sistemas tecnológicos para facilitar su labor diaria, por esto es relevante que se puedan tener espacios de conversación, concientización y formación, respecto a cómo protegerse en el entorno cibernético desde el rol de empleado. Te presentamos algunos puntos para resaltar en este acompañamiento:



1

Es común que se presenten diversas situaciones que afecten la operación de los colaboradores, por esto se deben establecer **canales de comunicación que permitan a los empleados reportar situaciones anómalas** para brindar atención oportuna a este tipo de casos y permitir que continúen con su operación diaria.

2

El uso de herramientas tecnológicas para combatir a los ciberdelincuentes que intenten comprometer a tu empresa, permite protegerla frente a gran cantidad de ataques. **Sin embargo, cuando las herramientas fallan, los empleados harán parte de esa primera línea de defensa y es allí cuando formarlos en la protección ante amenazas digitales, cobra importancia.** Podrás realizar estas formaciones por medio de estrategias sencillas que brinden información básica y valiosa a través de correo electrónico, formación presencial o virtual, para comprender los riesgos y así poder reaccionar frente a estos ataques, que son capaces de penetrar las barreras tecnológicas.

3

Quien no practica lo que aprende lo olvida, es por esto por lo que realizar mediciones y ejercicios prácticos de ciberseguridad a los empleados luego de haberlos formado, será esencial para permitir que el conocimiento entregado permanezca en ellos por un largo tiempo y de esta manera, poder proteger a las empresas desde su recurso más valioso, las personas.

Mediante estas recomendaciones, esperamos aportar a la gestión de la ciberseguridad en los esquemas de trabajo remoto en tu compañía, en pro de su fortalecimiento y la mitigación de amenazas a las que puede estar expuesta.