Tips para proteger la información de tu empresa en las nuevas modalidades de trabajo

El entorno digital representa un gran aliado para las empresas, sobre todo en épocas coyunturales como la actual. Sin embargo, también conlleva algunos factores de riesgo que pueden impactar la seguridad de la información, la cual es el ADN de todas las compañías y permite darles valor y forma a los objetivos estratégicos.

Por eso, desde el Centro de Protección Digital de SURA compartimos algunos tips y recomendaciones para proteger la información en estas nuevas dinámicas de trabajo.

01. Protección en las estaciones de trabajo

Habilita sistemas como antivirus o antimalware. Estos ayudan a proteger la información que se gestiona desde las estaciones de trabajo remoto. Ten en cuenta que debes mantenerlos actualizados para protegerte frente a las amenazas como, por ejemplo, la descarga de software malicioso mediante correos electrónicos o visitas a sitios web.

Utiliza sistemas para controlar la navegación. Estos pueden bloquear algunas páginas sospechosas, evitando que puedan abrirse si el colaborador, por error, intenta acceder a ellas y así, la información está protegida de los ciberdelincuentes.

Habilita sistemas de cifrado en los discos duros. Hazlo especialmente en portátiles o móviles, de manera que, si son hurtados, los datos permanezcan seguros.

Verifica la actualización de las aplicaciones utilizadas. Esto ayuda a mitigar los riesgos de tener un software desactualizado y vulnerable a los ataques cibernéticos.

02. Protección del correo electrónico

Usa sistemas para la protección frente a correo no deseado y malicioso. Algunos como AntiSpam y ATP (Protección de Amenazas Avanzadas) permiten filtrar los riesgos, evitando así que correos malintencionados puedan robar información o infectar las estaciones de trabajo.

03. Autenticación segura

Implementa y divulga una política de contraseñas seguras. Esta debe contemplar la indicación sobre contraseñas de mínimo 12 caracteres, que tengan mayúsculas, minúsculas, números y caracteres especiales. Evita el uso de palabras fáciles de adivinar y solicita un cambio periódico de las contraseñas.

Habilita el doble factor de autenticación. Conocido también como clave dinámica, aplica para cuentas de correo, redes sociales, VPN (Red Privada Virtual) y aplicaciones corporativas. Esto te ayudará en caso de robo de contraseñas, ya que el atacante necesitará un código adicional.

Visita nuestra sección Biblioteca experta y conoce la guía para contraseñas seguras y los manuales de configuración segura

Haz clic aquí

04. Acceso a servicios remotos corporativos

Implementa o fortalece una solución VPN (Red Privada Virtual). Esta opción permite a tus trabajadores conectarse directamente a la red corporativa y a las aplicaciones internas necesarias para realizar las labores, sin exponer más de lo necesario, evitando ampliar la superficie de ataque.

05. Seguridad en las aplicaciones

Cuenta con protocolos seguros para las comunicaciones. Puedes configurar las aplicaciones con protocolos como HTTPS para que la información viaje segura por la red sin que personas no autorizadas accedan y comprometan su confidencialidad.

Determina los permisos de acceso necesarios. Es importante que los trabajadores tengan acceso únicamente a los lugares donde ejecutarán sus labores, con el fin de prevenir la fuga de información y los permisos excesivos.

Haz pruebas periódicas de seguridad. Así podrás encontrar fallas de manera preventiva en la seguridad de las aplicaciones y corregirlas antes de publicarlas.

Utiliza sistemas de protección tipo WAF (Web Application Firewall). De esta manera, es posible proteger las páginas web de los ciberataques más comunes.

06. Ciber resiliencia

Realiza copias de seguridad para la información crítica. Con ello, disminuyes el impacto negativo de una pérdida, robo o secuestro de la información.

Revisa la capacidad de los canales de internet. El trabajo remoto, muchas veces representa un reto para las empresas en las capacidades de cómputo, almacenamiento y red. Por eso, debes monitorear constantemente el estado de estos indicadores para corregir o implementar planes de acción frente a estos problemas.

¡Aprende más con el Centro de Protección Digital SURA!

07. Cultura de ciberseguridad

Genera conciencia sobre la gestión de datos sensibles. Explica a tus colaboradores la importancia de evitar compartir información sensible, por ejemplo información financiera, usuarios y contraseñas, números telefónicos, historias clínicas. Además adviérteles sobre el uso redes públicas de WIFI, ya que no hay un control sobre ellas y son vulnerables a interceptaciones.

Establece canales de comunicación. Para que tus empleados puedan reportar alguna situación anómala o sospechosa que ponga en riesgo la información.

Capacita a tus empleados sobre los riesgos digitales. Es importante que ellos conozcan las amenazas de la red como correos maliciosos, suplantación de identidad, virus informáticos, entre otros, para garantizar la prevención, identificación y actuación frente a esos problemas.

Evalúa el nivel de preparación en temas de seguridad informática. Para esto, puedes utilizar tests, cursos virtuales o simulacros que fomenten una cultura reflexiva sobre los riesgos en la web y les dé la información necesaria para actuar correctamente.