Bogotá DC, 13 septiembre de 2023

**Asunto:** Situación Alerta Ciberseguridad de ataque a IFX Networks S.A.S

Señores entidades del Estado;

Desde el Comité Nacional de Seguridad Digital, se adelantó en las instalaciones de Presidencia, con presencia de MINTIC-COLCERT y CSIRT Presidencia y de manera virtual con presencia de algunas entidades afectadas, en atención al incidente presentado a la infraestructura de IFX, de tipo Ransomware; que presta servicios a las entidades del Estado y Organizaciones privadas en Latinoamérica, tomó la decisión de abrir de manera permanente el Puesto de Mando Unificado CIBER, a fin de hacer seguimiento sobre la gestión del mismo.

Así las cosas, si su entidad se vio afectada producto de este incidente, favor comunicarse con el CSIRT Presidencia al teléfono (601) 5629300 ext 3309, correo electrónico csirt@presidencia.gov.co con copia a los correos segdig-gtd@presidencia.gov.co ; contacto@colcert.gov.co.

Así mismo, nos permitimos reiterar las siguientes recomendaciones de seguridad digital, para que sean revisadas, validadas y aplicadas con el área respectiva de TI, a fin de mejorar la postura de seguridad independientemente si se vieron o no afectadas con el citado ataque y prevenir otro tipo de amenazas:

- No abrir correos ni mensajes de dudosa procedencia: Evita abrir correos electrónicos o mensajes de origen desconocido o sospechoso, ya que podrían contener malware o intentos de phishing.

- Desconfiar de los enlaces y archivos adjuntos en los mensajes o correos: Antes de hacer clic en un enlace o abrir un archivo adjunto, verifica la legitimidad del remitente y el contenido. Si tienes dudas, no lo hagas.

- Mantener actualizadas las plataformas de gestión administrativa y software de seguridad: Asegúrate de que todas las herramientas utilizadas, como Office, Windows, Adobe Acrobat, Oracle Java, y similares, estén actualizadas para protegerse contra vulnerabilidades conocidas.

- Mantener actualizadas sus plataformas de antivirus al día.

- Ser escépticos frente a ofertas, promociones o premios increíbles en Internet: Si algo parece demasiado bueno para ser verdad, probablemente lo sea. Mantén un nivel de escepticismo ante ofertas en línea que parezcan poco realistas.

- Prestar atención a los detalles en los mensajes y redes sociales: Examina cuidadosamente los mensajes y publicaciones en las redes sociales en busca de errores gramaticales o de ortografía, ya que estos pueden ser indicativos de intentos de estafa.

- Evaluar el bloqueo preventivo de los indicadores de compromisos reportados por el CSIRT: Si el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Informática) informa sobre indicadores de compromiso, considera bloquearlos o tomar medidas preventivas adecuadas.

- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas: Además de actualizar el software, asegúrate de que las soluciones de detección de amenazas estén actualizadas para proteger tu red.

- Revisar los controles de seguridad AntiSpam y SandBoxing: Asegúrate de que los controles de seguridad AntiSpam y SandBoxing estén configurados y funcionando correctamente para filtrar correos no deseados y archivos sospechosos.

- Concientizar a los usuarios sobre amenazas en la web: Educa a los usuarios de la organización sobre los peligros en línea, como el phishing y el malware, y fomenta prácticas seguras en línea.

- Verificar la autenticidad de los sitios web: Antes de ingresar información sensible en un sitio web, asegúrate de que sea oficial, cuente con certificados de seguridad válidos y sea de emisión legítima.

- Restringir el acceso a proveedores de red: Si una entidad ha otorgado acceso a la red a un proveedor externo, debe revisar y limitar ese acceso de manera oportuna.

- Realizar escaneos completos con el antivirus: Escanea regularmente todos los equipos con un antivirus actualizado para detectar y eliminar posibles amenazas.

- Verificar el rendimiento de Procesadores y Discos Duros: Monitoriza el rendimiento de hardware, como procesadores y discos duros, para detectar anomalías que podrían indicar problemas de seguridad.

- Revisar la integridad de los datos: Asegúrate de que los datos críticos estén intactos y no hayan sido comprometidos por amenazas de seguridad.

- Detectar incrementos injustificados en el tráfico de red: Establece alertas para identificar aumentos inesperados en el tráfico de red, lo que podría indicar un ataque o una intrusión.

Atentamente

**PMU CIBER**