Identificador
[COLCERT AD-0719-009]

05/08/2022

Advertencia de Seguridad Digital

[TLP: WHITE]

Recomendaciones de Seguridad

Posesión Presidente de la República 7 de agosto de 2022

Teniendo en cuenta la posesión del Presidente de la Republica de Colombia, a realizarse el próximo 7 de agosto de 2022, se recomienda a las entidades, tomar todas las consideraciones necesarias para proteger la infraestructura tecnológica y que de esta manera no sean vulnerados los sistemas que alojan información sensible, confidencial y que ayuda en la continuidad del negocio; de igual forma, se debe monitorear continuamente los componentes que hacen parte de la infraestructura para detectar actividades anómalas, así como usuarios inusuales que pueden estar exfiltrando información sin el conocimiento y autorización de la entidad.

Recomendaciones:

- Actualizar la matriz de riesgos de seguridad digital de la entidad y ajustar los controles para mitigar los riesgos.
- Establecer un procedimiento de *backups*, en donde disponga de por lo menos 3 copias y que se encuentren salvaguardados en sitio, fuera de sitio y en la nube. Es importante que dichas copias estén continuamente actualizadas a fin de contar con la información más reciente posible.
- Realizar un sondeo al servidor web a fin de identificar servicios que estén abiertos, que no se usen, obsoletos o sean considerados una amenaza de la seguridad (telnet y RDP).
- Actualizar y parchar sistemas operativos, antivirus y programas con las últimas actualizaciones, NO use bajo ningún motivo aplicaciones obsoletas que ya no cuenten con soporte técnico.
- Proteger los activos críticos, siguiendo el modelo de seguridad de cero confianza (*Zero Trust*).
- Complementar el servicio de antivirus con servicios de Detección y respuesta de punto final (EDR), Detección y respuesta extendidas (XDR)
- Validar si los agentes de antivirus se encuentran actualizados y si están reportando a la consola.
- Implementar *Web Application Firewall* (WAF), para protección de las aplicaciones web.
- Identificar las aplicaciones y servidores frente a cada proceso (misional, estratégico, soporte y mejora).
- Actualizar el diagrama y topología de la infraestructura tecnológica de la entidad.

- Realizar las actualizaciones de Vulnerabilidad Productos Windows (CVE-2022-22047) - *Client Service Runtime Process* – CSRSS.
- Validar continuamente los funcionarios que han cambiado de cargo o han sido desvinculados de la entidad, con el propósito de suspender los accesos a las aplicaciones y servicios de red.
- Cambiar credenciales de administradores de aplicaciones, servidores, bases de datos, plataformas de seguridad.
- Establecer una política de control de acceso, que establezca el cambio de contraseñas a usuarios por lo menos cada 45 días.
- Restringir el acceso de la red de VPN a aplicaciones y servicios críticos de la entidad - modelo de seguridad de cero confianza (*Zero Trust*).
- Establezca un plan de acción para la actualización de sistema *Legacy* o sistema heredado.
- Establecer un equipo de respuesta a incidentes de seguridad de la información, así como el procedimiento para gestión de los incidentes en la entidad - Resolución 500 del 2021.
- Reportar los incidentes de seguridad digital al CSIRT Gobierno al buzón de correo csirtgob@mintic.gov.co, de acuerdo a lo establecido en la Resolución 500 del 2021.
- Leer los boletines de alerta y advertencia elaboradores por el COLCERT, los cuales pueden ser consultados en la URL https://bit.ly/BoletinesCOLCERT
- Actualizar los contactos técnicos de los CIO y CISO de la entidad, diligenciado en siguiente formulario - https://forms.office.com/r/6pRjYzEfds
- Seguir la cuenta de Twitter del @COLCERT para recibir de manera oportuna información de seguridad digital en el país.

Canales de Atención

Si tiene alguna consulta técnica, puede comunicarse con CSIRT Gobierno de tratarse de una entidad del Estado, o con COLCERT si pertenece a cualquier otro sector de la economía, a través de los siguientes canales:

Bogotá: +57 601 344 22 22
Línea Gratuita Nacional: 018000952525 Opción 2

contacto@colcert.gov.co,
csirtgob@mintic.gov.co

@colCERT

Hechos QUE CONECTAN