Identificador
[COLCERT- AD-0613- 012]

2023/06/13

Advertencia de Seguridad Digital

TLP:CLEAR

RECOMENDACIONES DE SEGURIDAD DIGITAL PARA LAS ENTIDADES PUBLICAS Y PRIVADAS

Contexto:

Teniendo en cuenta la implementación de infraestructura tecnología en las diferentes iniciativas transformación digital que vienen implementado las entidades públicas y privadas a nivel nacional y territorial, las cuales aumentan la huella digital y con ésta la superficie de exposición, adicionalmente los actores de amenazas locales, regionales y globales días a día vienen desarrollando e implementado nuevas métodos y estrategias para atacar a las entidades y causar afectación a los sistemas de información con el propositivo de buscar inicialmente un beneficio económico, generar desconfianza y alterar el orden institucional del Estado.

Así las cosas, las siguientes recomendaciones de seguridad, están orientadas a que las entidades las revisen y las implementen con el propósito de mejorar la postura de seguridad digital y evitar incidentes de seguridad digital que afecte la disponibilidad de la información, la reputación entidades y sobre todo la perdida de información principalmente de sus procesos misionales.

Acciones inmediatas

- Implementar el doble factor de autenticación en las cuentas de correo. En el siguiente link encontrara información sobre la configuración de MFA en Office 365:

https://learn.microsoft.com/es-es/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide

- Evitar a toda costa compartir credenciales (usuario/contraseña) de cuentas de correo corporativas, así mismo evitar utilizar éstas en redes sociales, apertura de servicios en línea, servicios financieros externos a la entidad, entre otras. En el siguiente link encontrara una herramienta en línea para crear contraseñas seguras.

https://support.microsoft.com/es-es/topic/use-generador-de-contrase%C3%B1as-para-crear-contrase%C3%B1as-m%C3%A1s-seguras-en-microsoft-edge-e9247e35-684b-4114-bb5e-fdea3e4ae3ff#:~:text=C%C3%B3mo%20funciona%20el%20generador%20de,segura%20en%20un%20men%C3%BA%20desplegable.

En caso de no implementar Múltiple factor de autenticación, establecer una política de generación, cambio, reutilización de credenciales de usuarios y cambio periódico de las mismas.

- Recomendar a los usuarios de la entidad, no utilizar los buzones de correo corpotrativo, en servicios y redes sociales personales.
- Actualizar la matriz de riesgos y ajustar los controles para proteger activos vulnerables, sistemas y aplicaciones legadas.
- Actualizar a su última versión los sistemas de gestión de contenido CMS (Content Management System) y realizar el afinamiento a la configuración para evitar exponer información de configuración a través de directorios.
- Mantener actualizados los sistemas operativos de computadores y servidores, con las actualizaciones críticas y de seguridad, así como tener políticas de endurecimiento (hardening), siguiendo buenas prácticas para minimizar la materialización de riesgos.
- Validar el despliegue de los agentes de **antivirus** en computadores y servidores, en la consola para validar el cubrimiento total de la infraestructura tecnológica de la entidad.
- Establecer y operacionalizar procedimientos detallados para la generación de copias de seguridad
- Realizar actualización de seguridad a sistemas operativos a computadores, servidores, equipos activos de red y seguridad informática.
- Realizar un monitoreo a los eventos de seguridad y logs de las plataformas (FW, IDS/IPS, DA, AV, WAF, Balanceador, BD, SW) para identificar Indicadores de Amenaza – IoA.
- Implementación protocolo autenticación como SPF, DKIM y DMARC para su dominio de correo.

Recomendaciones Generales

- Establecer una política de gestión de contraseñas.
- Establecer una política de control de acceso.
- Actualizar el inventario de activos de información incluyendo los de nube.
- Establecer un plan de capacitación y concienciación para la entidad.
- Actualizar la matriz de riesgos de la entidad contemplando las infraestructuras on-premises y de nube.
- Recomendar a los usuarios no descargar software y aplicaciones ilegales, que puedan afectar la seguridad de la infraestructura tecnológica de la entidad.
- Recomendar a los usuarios no conectarse a redes inalámbricas Wi-Fi abiertas, que puedan capturar credenciales y exfiltrar información.
- Realizar análisis de vulnerabilidades plataformas expuestas en internet y realizar planes de mitigación de éstas.
- Actualizar y operacionalizar el Plan de Recuperación ante Desastres DRP.
- Realizar pruebas de continuidad de la operación, para cada una de las copias de seguridad generadas.

- Actualizar o implementar soluciones de antivirus para tener mayor visibilidad como soluciones EDR (Endpoint Detection and Response) para proteger dispositivos y XDR (Extensive Detection and Response) para proteger redes, aplicaciones y datos
- Implementación de DNSSEC, en su sistema de Dominio, para garantizar la confiabilidad y credibilidad de éste en la entidad.
- Revisar, atender y gestionar los Boletines y Alertas emitidos por las instancias Ciber del Estado, así como de organismos internacionales en lo respectivo a vulnerabilidades críticas y altas que se deban atender, procurando tomar las medidas necesarias para atender las recomendaciones que se dan al respecto

Cumplimiento normativo de Seguridad Digital

- Dar cumplimiento al habilitador transversal de seguridad y privacidad, establecido en la Política de Gobierno Digital - Decreto 767 de 2022, con la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI.
- Dar cumplimiento a lo establecido en la Resolución 500 del 2021 del MinTIC, sobre la implementación de una estrategia de seguridad digital para la entidad, así como la implantación de un procedimiento de gestión de incidentes.
- Establecer frente a los documentos que genera, obtiene, adquiera, transforme y controle la entidad, que éstos cuente con las siguientes características; Información, pública, pública clasificada y pública reservada, lo anterior en cumplimiento a la ley 1712 del 2014
- Establecer la política de protección de datos personales – Ley 1581 del 2012. que garantice la protección de los datos sensibles de los usuarios.

Referencias

https://learn.microsoft.com/es-es/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide
https://support.microsoft.com/es-es/topic/use-generador-de-contrase%C3%B1as-para-crear-contrase%C3%B1as-m%C3%A1s-seguras-en-microsoft-edge-e9247e35-684b-4114-bb5e-fdea3e4ae3ff#:~:text=C%C3%B3mo%20funciona%20el%20generador%20de,segura%20en%20un%20men%C3%BA%20desplegable.

Canales de Atención

Si tiene desea reportar un incidente de seguridad digital, puede comunicarse con el COLCERT, 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