**Política:** Seguridad Digital

1. ¿La entidad tiene designado un responsable de la Seguridad Digital - (Ciberseguridad)?



Selección única

Sí, y pertenece a la planta de personal Sí, es un contratista

No tiene a nadie designado

Código: SDI200

1. Indique el porcentaje del presupuesto total asignado a la Seguridad Digital (Ciberseguridad), para la protección de los datos digitales en la entidad (Costos de personal, herramientas, IPS/IDS, firewall, Antivirus, EDR, servidores, sistemas, licencias etc.): 0.6%

Código: SDI201

Abierta numérica

1. ¿La entidad garantiza la continuidad del soporte, actualización y mantenimiento de las herramientas, plataformas, licencias, servicios y sistemas de información que hacen parte de la infraestructura tecnológica de la entidad?



Selección única

Código: SDI202

El total de la infraestructura tecnológica de la entidad se encuentra cubierta con el soporte, actualización y mantenimiento requerido para su operación

 La infraestructura tecnológica se encuentra parcialmente cubierta; sin embargo, ya se tiene incluido en el plan de actualización del área de TI para el cubrimiento total de la infraestructura

 La infraestructura tecnológica se encuentra parcialmente cubierta por el soporte, actualización y mantenimiento requerido, y aún no se tiene contemplada dicha actualización

La infraestructura tecnológica de la entidad no cuenta con soporte, actualización y mantenimiento requerido para su operación



1. ¿La entidad contó con una política o lineamientos definidos y documentados para la generación y restauración de copias de respaldo de la información?



Selección única

Código: SDI204

Sí, y cuenta con las evidencias:

No

1. Respecto a las copias de respaldo de la información, del software e imágenes de los sistemas, la entidad:



Selección múltiple

Código: SDI205

Tiene documentados e implementados procedimientos para copias de respaldo y de restauración

Los equipos que realizan las copias de respaldo se encuentran en entorno lógico separados e independiente a la red de servidores y computadores

Las copias de respaldo son almacenadas en un lugar aislado, en un segmento diferente de red a la de servidores y equipos



 Se realizan pruebas de respaldo a las copias de seguridad de la información de los aplicativos misionales, estratégicos, soporte y de mejora, de manera programada para asegurar la disponibilidad de los datos en caso de Ransomware, de manera coordinada con los responsables del proceso

 Ninguna de las anteriores

1. Para asegurar la continuidad de la operación de los procesos, en la entidad:

Código: SDI206



Selección múltiple

Se cuenta con un Plan de Recuperación de Desastres DRP, definido, documentado e implementado para todos los procesos

 Se cuenta con un Plan de Continuidad del Negocio BCP, definido, documentado e implementado para los procesos críticos y misionales

Ninguna de las anteriores



1. ¿La entidad realizó pruebas de recuperación de información y continuidad de los sistemas de información críticos en la vigencia evaluada?



Selección única

Código: SDI207

Si, realizó pruebas de recuperación de la información a todos los sistemas críticos y misionales

Si, pero de manera parcial. Realizó pruebas de recuperación a algunos de los sistemas críticos y misionales

No realizó pruebas de recuperación de información y continuidad de los sistemas de información críticos y misionales

1. ¿La entidad identificó y gestionó los riesgos de seguridad digital (Ciberseguridad) de sus infraestructuras on premise?

Selección única

Código: SDI208

Infraestructuras on premise: hace referencia a la instalación de un sistema en una ubicación física, es decir, un Identificó los riesgos, pero no se han gestionado



Identificó y gestionó los riesgos

No ha identificado los riesgos de sus infraestructuras on premise

1. ¿La entidad identificó y gestionó los riesgos de seguridad digital (Ciberseguridad) en los servicios de Nube Pública/Privada que utiliza?

Selección única

Código: SDI209

Los servicios de nube: son infraestructuras, plataformas o sistemas de software que alojan los proveedores externos Identificó y gestionó los riesgos



Identificó los riesgos, pero no los ha gestionado

No ha identificado los riesgos de los servicios de Nube Pública/Privada No ha utilizado servicios de Nube Pública/Privada

1. ¿La entidad contó con equipos de seguridad perimetral para su infraestructura on premise?

Código: SDI210

Selección única

Infraestructuras on premise: hace referencia a la instalación de un sistema en una ubicación física, es decir, un Si, con un firewall licenciado y con soporte



Si, con un firewall, pero sin licenciamiento ni soporte

No se contó con firewall

1. ¿La entidad contó con soluciones antivirus para sus servidores físicos, servidores virtuales y los computadores?



Selección única

Código: SDI211

Si, se contó con antivirus licenciado y con soporte para todos los servidores físicos, virtuales y computadores Parcialmente. Se contó con antivirus licenciado y con soporte, pero solo para algunos de los servidores físicos, virtuales y computadores

 Se contó con antivirus para los servidores físicos, virtuales y computadores, pero no se contó con licenciamiento ni soporte

No se contó con antivirus



1. ¿La entidad realizó análisis de vulnerabilidades de seguridad a los activos de información a su infraestructura On Premise en la vigencia evaluada?



Selección única

Código: SDI212

Si, lo realizó. Registre la fecha de entrega del informe del análisis: sept 2024

No

1. ¿La entidad realizó análisis de vulnerabilidades de seguridad a los activos de información de su infraestructura en Nube Pública/Privada en la vigencia anterior?



Selección única

Código: SDI213

Sí. Registre la fecha de entrega del informe del análisis: sept de 2024

No

1. ¿La entidad realizó análisis de vulnerabilidades para Portal Web, Sede electrónica y Servicios expuestos en Internet en la vigencia anterior?



Selección única

Código: SDI214

Sí, y cuenta con las evidencias:

No

1. ¿La entidad se cercioró que los proveedores y contratistas cumplieran con las políticas o lineamientos internos de seguridad digital (Ciberseguridad)?



Selección única

Código: SDI216

Sí, y cuenta con las evidencias:

No se verificó el cumplimiento

La entidad no tiene lineamientos internos de ciberseguridad

1. ¿La entidad implementó un sistema para el cumplimiento de la ley 1581 de 2012 -Ley de Protección de Datos Personales?



Selección única

Código: SDI219

Sí, y cuenta con las evidencias: No se ha implementado

1. ¿La entidad estableció e implementó un procedimiento para la gestión de incidentes de seguridad digital (Ciberseguridad)?



Selección única

Código: SDI220

Ha sido establecido, documentado e implementado e incluye la notificación a las autoridades pertinentes (CSIRT Gobierno / COLCERT)



Ha sido establecido, documentado e implementado No lo ha establecido

1. Respecto de los incidentes de seguridad digital (Ciberseguridad) durante la vigencia evaluada indique:



Selección múltiple

Código: SDI222 unoCuántos de esos incidentes fueron clasificados como Muy Graves y Graves: 9Cuántos de esos incidentes fueron clasificados como Menos Grave y Menor:

No se presentó ningún incidente de seguridad digital durante la vigencia evaluada

1. ¿La entidad reportó los incidentes de seguridad digital (Ciberseguridad) acorde con lo establecido en la resolución 500 de 2022 del Ministerio de Tecnologías de la Información- MINTIC - COLCERT?



Selección múltiple

Código: SDI223

Reportó los incidentes de seguridad digital clasificados como "muy graves y graves" (1)

Comunicó los incidentes de seguridad digital clasificados como "menos graves y menor" (9)

La entidad no reportó los incidentes 1

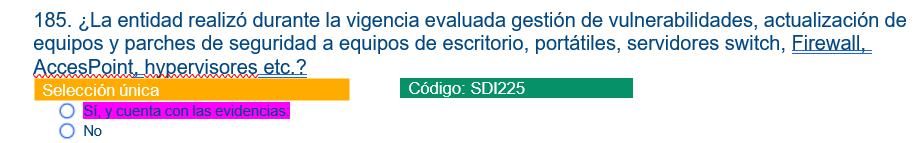
1. ¿La entidad tiene licenciados los sistemas operativos de todos los equipos de escritorio, portátiles y servidores?



Selección única

Código: SDI224

Sí, y cuenta con las evidencias:

No, los sistemas operativos no tienen licencia

1. ¿La entidad tiene implementado métodos de autenticación del correo electrónico como DMARC, DKIM y SPF, para seguridad del correo electrónico y garantizar la autenticidad de los remitentes?



Selección única

Código: SDI226

Sí, y cuenta con las evidencias:

No, la entidad no tiene implementados métodos de autenticación del correo electrónico