Radicado DADEP No. 20221300082023

**20221300082023*

Bogotá D.C, 30-11-2022
Código y sigla de la dependencia (tamaño 8)

**MEMORANDO**

**PARA: DIANA ALEJANDRA RODRÍGUEZ CORTÉS**
Directora

**DE: ALLAN MAURICE ALFISZ LÓPEZ**
Jefe Oficina de Control Interno

**ASUNTO:** Remisión Informe Seguimiento ISO 27001:2013

La Oficina de Control Interno en ejercicio de sus funciones y roles asignados en el Decreto 648 de 2017 y en cumplimiento del Plan Anual de Auditoría 2022, se permite remitir el informe de seguimiento ISO 27001:2013 relacionado con la Seguridad de la Información. Adicionalmente, como control preventivo, esta oficina realizará durante el primer semestre del año 2023 monitoreo a las recomendaciones planteadas en dicho informe.

Cordialmente,

**ALLAN MAURICE ALFISZ LÓPEZ**

Anexo: Informe de Seguimiento en 20 folios

Copia: Syrus Asdrúbal Pacheco Vergel, Jefe OTIC
Elaboró: Albeiro Rizo
Revisó y Aprobó: Allan Maurice Alfisz
Fecha: 29 de noviembre de 2022
Código: 1308515

DEPARTAMENTO ADMINISTRATIVO DE LA DEFENSORÍA DEL ESPACIO PÚBLICO

**DEPARTAMENTO ADMINISTRATIVO DE LA DEFENSORÍA DEL ESPACIO PÚBLICO**

**OFICINA DE CONTROL INTERNO**

# Informe
# SEGUIMIENTO SISTEMA DE SEGURIDAD DE LA INFORMACIÓN (ISO 27001:2013)

**Bogotá D. C., noviembre de 2022**

## Contenido

**INTRODUCCIÓN** ..... **6**

**1. OBJETIVOS** ..... **6**

**1.1 OBJETIVO GENERAL** ..... **6**

**1.2 OBJETIVOS ESPECÍFICOS** ..... **6**

**2. ALCANCE** ..... **6**

**3. CRITERIOS** ..... **7**

**4. INFORME DE GESTIÓN Y RESULTADOS** ..... **7**

**4.1 SOLICITUD DE INFORMACIÓN** ..... **7**

**4.2 ANÁLISIS DE LA INFORMACIÓN** ..... **7**

4.2.1 Objetivo de control A.6.1.3 (Contacto con las autoridades) ..... 7
4.2.2 Objetivo de control A.6.2.1 (Política para dispositivos móviles) ..... 8
4.2.3 Objetivo de control A.6.2.2 (Teletrabajo) ..... 11
4.2.4 Objetivo de control A.8.3.1 (Gestión de medios removibles) ..... 12
4.2.5 Objetivo de control A.9.1.1 (Política de control de acceso) ..... 13
4.2.6 Objetivo de control A.9.4.5 (Control de acceso a códigos fuente de programas) ..... 14
4.2.7 Objetivo de control A.11.1.4 (Protección contra amenazas externas y ambientales) ..... 16
4.2.8 Objetivo de control A.12.1.4 (Separación de los ambientes de desarrollo, pruebas y operación) ..... 18
4.2.9 Objetivo de control A.14.2.2 (Procedimientos de control de cambios en sistemas) ..... 18
4.2.10 Objetivo de control A.16.1.6 (Aprendizaje obtenido de los incidentes de seguridad de la información) ..... 19
4.2.11 Consolidación objetivos de control ..... 20

**5. CONCLUSIONES** ..... **21**

**6. RECOMENDACIONES** ..... **21**

## Listado de tablas

Tabla No. 1. Contacto con entidades distritales ..... 7
Tabla No. 2. Verificación de aplicación de los controles ..... 20

## Listado de imágenes

Imagen No. 1. Segmentación de la red (WiFi usuarios Corporativos/Visitantes) ..... 8
Imagen No. 2. Control Access Point usuario Invitados ..... 9
Imagen No. 3. Control acceso sitio web pornográfico (usuario Corporativo - PC) ..... 9
Imagen No. 4. Control acceso sitio de loterías (usuario Corporativo – Vía PC) ..... 10
Imagen No. 5. Control acceso sitio web pornográfico (usuario Invitado – Vía celular) ..... 10
Imagen No. 6. Acceso a juegos en línea ..... 11
Imagen No. 7. Acceso a carpeta compartida ..... 12
Imagen No. 8. Acceso a repositorios GIT ..... 14
Imagen No. 9. Repositorios habilitados para ingenieros OTIC ..... 15
Imagen No. 10. Repositorios de código fuente ..... 15
Imagen No. 11. Control de ataques maliciosos ..... 16
Imagen No. 12. Bloqueo de sitios inseguros ..... 17
Imagen No. 13. Registro de modificaciones aplicativo SUMA+ ..... 19

## INTRODUCCIÓN

La Oficina de Control Interno (OCI), en el marco de las funciones constitucionales y legales atribuidas, especialmente las estipuladas en los artículos 209 y 269 de la Constitución Política de Colombia, la Ley 87 de 1993, la Ley 80 de 1993, el Decreto 1082 de 2015 y en cumplimiento del Plan Anual de Auditoría 2022, adelantó el seguimiento a la seguridad de la información según la norma ISO 27001:2013, con el fin de verificar el cumplimiento de los controles indicados en Anexo A (Objetivos de control y Controles de referencia) de la citada norma.

La ISO 27001:2013 ofrece un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI) con el fin de proporcionar confidencialidad, integridad y disponibilidad continuada de la información; a través de la identificación y mitigación de los riesgos que eventualmente podrían afectar la información, evitando que se materialicen.

## 1. OBJETIVOS

### 1.1 OBJETIVO GENERAL

Verificar la gestión que realiza la Oficina de Tecnologías de la Información y Comunicaciones (OTIC) a la seguridad de la información, en el marco de la norma ISO 27001:2013.

### 1.2 OBJETIVOS ESPECÍFICOS

1. Evaluar los controles aplicados por la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), conforme al Anexo A: Objetivos de control y controles de referencia, de la citada norma.

2. Evaluar el control de acceso a sitios en Internet no autorizados.

## 2. ALCANCE

El seguimiento llevado a cabo por la Oficina de Control Interno contempló las actividades desarrolladas por la OTIC con corte al 31 de agosto de 2022, para algunos de los controles de la norma ISO/IEC 27001:2013, Anexo A: Objetivos de control y controles de referencia, tales como: Organización interna, Dispositivos móviles y Teletrabajo, Manejo de medios, Requisitos del negocio para control de accesos, Control de acceso a sistemas y aplicaciones, Áreas seguras, Procedimientos operacionales y responsabilidades, Seguridad en los

procesos de desarrollo y de soporte, Gestión de incidentes y mejoras en la seguridad de la información.

## 3. CRITERIOS

Se utilizó como criterio la Norma Técnica Colombiana NTC-ISO-IEC 27001:2013, Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

## 4. INFORME DE GESTIÓN Y RESULTADOS

### 4.1 SOLICITUD DE INFORMACIÓN

- A través del memorando No. 20221300076443 del 04/11/2022, se solicitó a la OTIC información con las evidencias correspondientes, relacionada con el sistema de seguridad; con plazo de entrega del 11/11/2022.

- La OTIC allegó mediante memorando No. 20221400078193 del 11/11/2022, la respuesta solicitada y entregó los soportes correspondientes en carpetas compartidas en OneDrive.

### 4.2 ANÁLISIS DE LA INFORMACIÓN

Con base en las respuestas allegadas por la OTIC se realizó el siguiente análisis de la información y de las evidencias recibidas.

#### 4.2.1 Objetivo de control A.6.1.3 (Contacto con las autoridades)

Las entidades del Distrito Capital con las que el Departamento Administrativo de la Defensoría del Espacio Público (DADEP) tiene contacto en temas de seguridad de la información, se observan en la tabla No. 1.

**Tabla No. 1. Contacto con entidades distritales**

| Entidad distrital | Tema | Canal de comunicación |
|---|---|---|
| Alta Consejería Distrital para las TIC | Talleres ComparTIC Bogotá | Reuniones periódicas presenciales |
| | Ruta de formación en Ciberseguridad | Capacitación virtual |
| | Grupo de Seguridad y Ciberseguridad Distrital | Mensajes a través de chat |
| Mesa de Infraestructuras Críticas del Distrito | Infraestructuras Críticas del Distrito | Reuniones periódicas presenciales |

Fuente: OTIC - Elaboración OCI

La Oficina de Control Interno evidenció la participación de la OTIC en las siguientes actividades:

- Taller: "Gestión y respuesta de ciberataques… ¡Sin morir en el intento!", el 25/08/2022.
- Asistencia por parte del oficial de seguridad de la información a la 1a. Mesa de Infraestructura Crítica del Distrito, el 08/08/2022.
- Generalidades de la protección de datos personales, 24/03/2022.
- Taller: "Seguridad Digital - Modelo de Seguridad y Privacidad de la Información - MSPI", el 24/02/2022.
- Inducción Seguridad Digital y Protección de Datos Personales, febrero de 2022.
- Documento: Global Threat Report (Informe de amenazas globales), 2021.

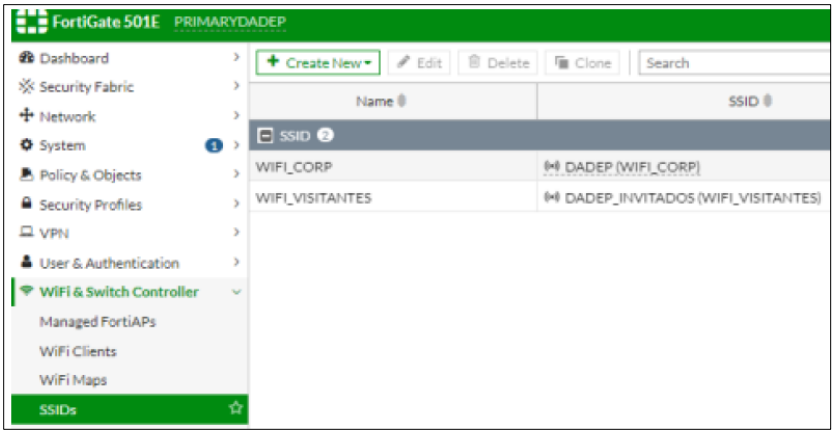
Para los demás archivos recibidos no fue posible identificar las fechas de celebración de las actividades relacionadas con seguridad de la información o algunas estaban por fuera del alcance del seguimiento.

En general, se destaca la asistencia de la OTIC a eventos en temas relacionados con la seguridad de la información, tales como, gobierno y seguridad digital, ciberataques y protección de datos personales, lo que coadyuva a obtener el conocimiento y las habilidades necesarias para enfrentar el impacto de eventuales riesgos que afecten la continuidad del negocio.

### 4.2.2 Objetivo de control A.6.2.1 (Política para dispositivos móviles)

El uso de dispositivos móviles en la entidad se realiza por conexiones WiFi, que permite el acceso a los servicios de la entidad, restringido por tipo de usuario: corporativo o visitante, quienes a través de autenticación ingresan a la red (ver imagen No. 1).

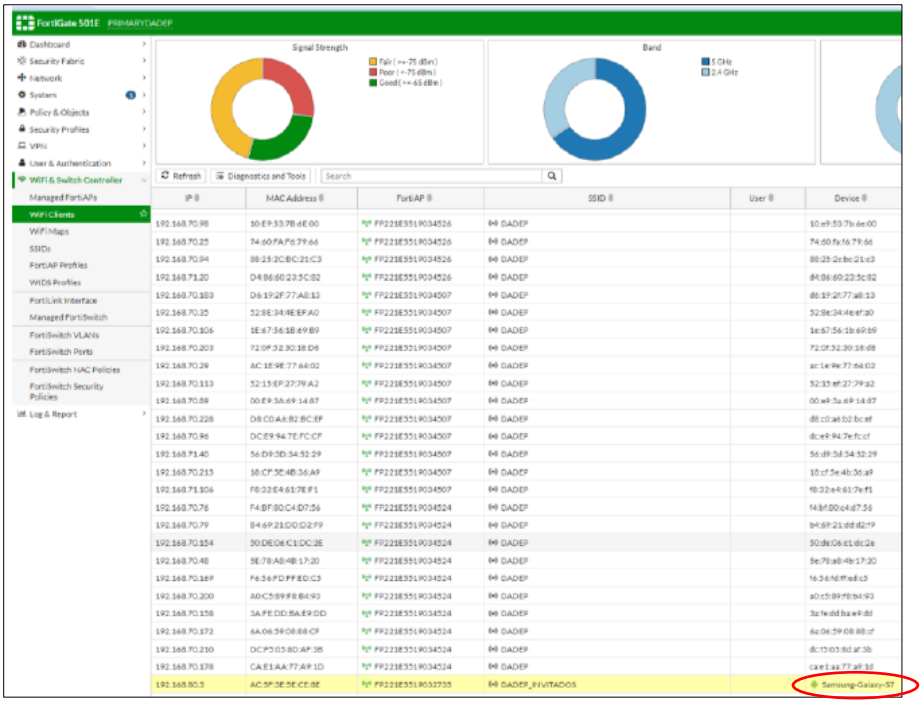
**Imagen No. 1. Segmentación de la red (WiFi usuarios Corporativos/Visitantes)**




Fuente: OTIC

En la imagen No. 2 se evidenció que el control de los Access Point se hace directamente en el firewall donde se mantiene monitoreado el tráfico, donde un usuario Invitado utilizó para ingresar a la red un celular Samsung Galaxy S7.

**Imagen No. 2. Control Access Point usuario Invitados**




Fuente: OTIC

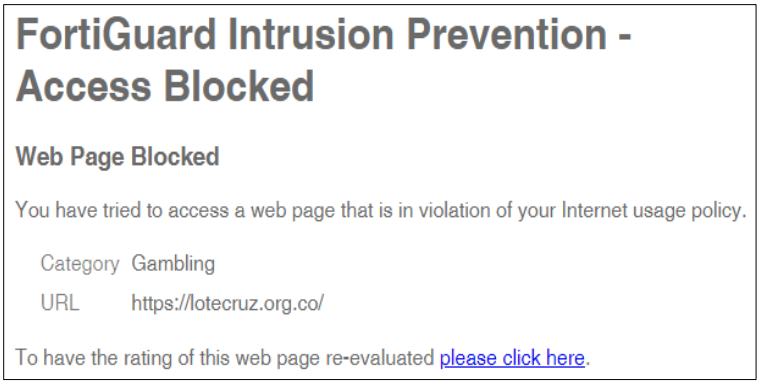
Adicionalmente, para la seguridad perimetral se utilizan dispositivos WAF (hardware o software que protegen los servidores de aplicaciones web de determinados ataques específicos en Internet) para inspeccionar el tráfico entrante y saliente de la red.

La Oficina de Control Interno intentó consultar, desde un computador de escritorio, un sitio de contenido pornográfico y de loterías, obteniendo como respuesta la negación del servicio. Ver imagen No. 3 y No. 4.

**Imagen No. 3. Control acceso sitio web pornográfico (usuario Corporativo - PC)**

Fuente: OTIC

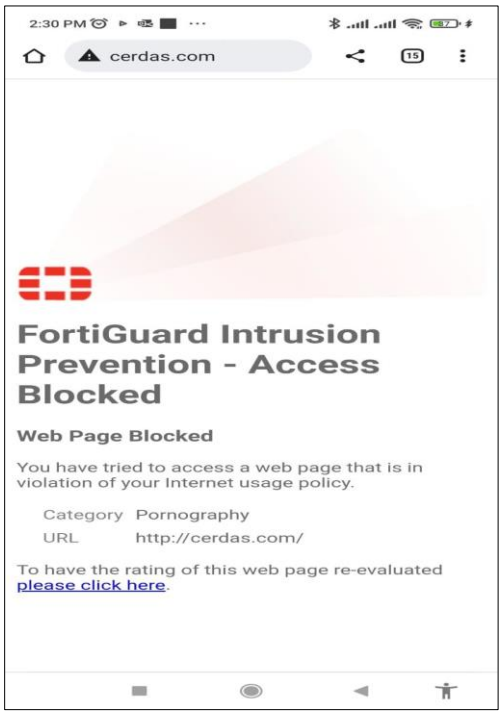
**Imagen No. 4. Control acceso sitio de loterías (usuario Corporativo – Vía PC)**




Fuente: OTIC

La imagen No. 5 muestra un intento de acceso de un usuario Invitado, por medio de un dispositivo móvil conectado a la red WiFi, a una página pornográfica.

**Imagen No. 5. Control acceso sitio web pornográfico (usuario Invitado – Vía celular)**

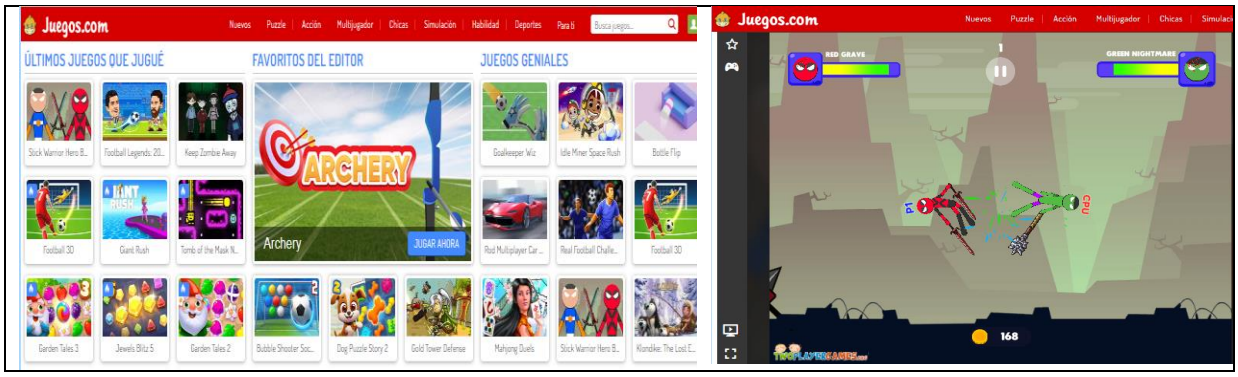



Fuente: OTIC

Lo anterior, evidenció la efectividad del control realizado por el sistema de seguridad perimetral que restringe el acceso a sitios no autorizados, que evita el riesgo eventual del ingreso de malware (software malicioso) en los computadores de la entidad.

No obstante, al consultar páginas de juegos en línea como Juegos gratis - Juega online en juegos.com, el acceso fue exitoso, lo que indica que se debe fortalecer el control de ingreso a este tipo de sitios web. Ver imagen No. 6.

**Imagen No. 6. Acceso a juegos en línea**




Fuente: Internet

### 4.2.3 Objetivo de control A.6.2.2 (Teletrabajo)

Para el personal de la entidad que labora en modalidad de teletrabajo, en cuanto a la protección de la información accesada, procesada o almacenada, según lo estipulado en el Manual de políticas operativas específicas de seguridad y privacidad de la información, específicamente la Política de Acceso Remoto, se tienen implementadas las siguientes medidas de seguridad:

- Definición de los canales y restricciones para accesar remotamente los recursos TIC del DADEP.

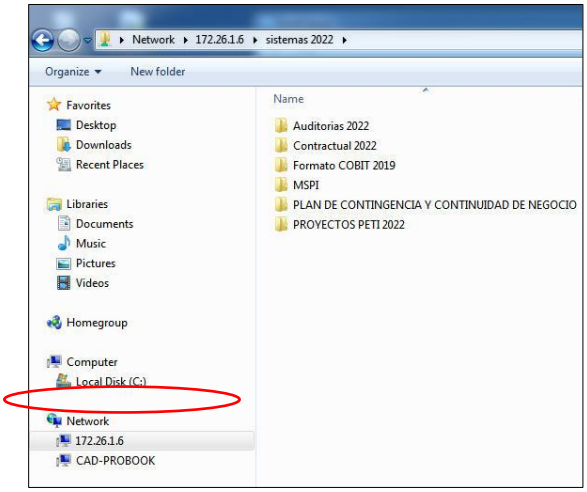
- Utilización como canal remoto de acceso, de la tecnología VPN (Virtual Private Network), cuya aprobación debe tener el visto bueno del jefe inmediato, del jefe de la OTIC y del oficial de seguridad de la información.

- La VPN garantiza el acceso únicamente a los usuarios autorizados y exclusivamente a los recursos de red asignados según el perfil.

- La actividad ejecutada por el personal remoto queda registrada en archivos logs.

Se evidenció la creación de una carpeta llamada *ejemplo 2* a la que únicamente tiene permisos el jefe de la OTIC, el oficial de seguridad intentó accederla, pero el control no lo permitió; lo anterior indica que se debe contar con los perfiles debidamente autorizados para poder realizar la consulta. La imagen No. 7 muestra acceso exitoso a la carpeta que si tiene permiso el oficial de seguridad.

**Imagen No. 7. Acceso a carpeta compartida**




Fuente: OTIC

### 4.2.4 Objetivo de control A.8.3.1 (Gestión de medios removibles)

Con respecto a la gestión de la información almacenada en medios removibles, la OTIC realiza en general los siguientes pasos, en caso de salvaguardar los datos:

1. Solicitud (ticket) del usuario en el Sistema de Gestión de Servicios.
2. La OTIC analiza la necesidad de respaldar la información del medio removible.
3. La OTIC restaura en el equipo de cómputo del usuario la copia respaldada.
4. El usuario de conformidad acepta la restauración de la copia respaldada.
5. La OTIC borra la información del medio removible y lo dispone para darlo de baja.

Con dicho procedimiento se garantiza que los datos almacenados en medios removibles, por obsolescencia o daño, sean borrados y restaurados en otros dispositivos para ser utilizados nuevamente por parte de los usuarios.

Se evidenció el caso del ticket No. 6061:

<u>Descripción</u>: "…revisar el equipo de cómputo, desde esta mañana el equipo prende pero no tiene sistema operativo…"

<u>Diagnóstico OTIC:</u>

- Disco duro dañado
- Las unidades de setup no reconocen el disco, es imposible recuperar la información, el disco no tiene arreglo.
- Se realizaron cuatro (4) métodos para poder recuperar la información y no fue posible.

Acciones OTIC:

- Cambiar el disco duro
- Instalar software

En situaciones como la descrita en el ticket No. 6061, técnicamente no fue posible recuperar los datos del disco duro dañado, pero desde el punto de vista de la seguridad de la información esta no quedó a disposición ni en riesgo de ser utilizada. Cabe anotar, que la entidad adquirió Microsoft 365, herramienta que ofrece almacenamiento en la nube a través de OneDrive o SharePoint, por lo tanto, los usuarios deben gestionar su información institucional en estos sitios y no en el disco duro local, para evitar pérdida de datos.

### 4.2.5 Objetivo de control A.9.1.1 (Política de control de acceso)

El acceso al Centro de Cómputo del DADEP por parte de los proveedores de tecnología para realizar mantenimientos preventivos o correctivos a la infraestructura de TI, está definido en el *Manual de políticas operativas específicas de seguridad y privacidad de la información*, específicamente la *Política de seguridad física y del entorno del centro de datos*, dentro de los que se encuentran:

- Registro en la planilla de control de acceso
- Control biométrico
- La presencia de terceros siempre debe hacerse en presencia de funcionarios o contratistas autorizados de la Oficina de Tecnología y las Comunicaciones

En la *Política de seguridad física y del entorno del centro de datos*, no se estipula acceso diferencial para proveedores de tecnología, es decir, tienen el mismo tratamiento de ingreso de funcionarios y contratistas de la entidad.

Se evidenció el ingreso al Centro de Cómputo por parte de las personas autorizadas (Jefe OTIC y Líder de Infraestructura de TI) a través de acceso biométrico y de la tarjeta RFID. Se intentó el ingreso con personal diferente a las autorizadas, siendo el resultado no exitoso.

En cuanto al ingreso al Centro de Cómputo por parte de proveedores de TI, se evidenció el diligenciamiento del formato No. 127-FORGI-10 (Control de acceso al centro de cómputo), con empresas como STS, ETB, ORACLE y ADSUM, entre otras, que hicieron visitas en los periodos de febrero a octubre de 2021 y de enero a agosto de 2022.

Cabe resaltar, que se identificó discordancia entre la denominación del Centro de Datos y del Centro de Cómputo en diferentes documentos, situación que podría causar confusión en la conceptualización de dichos términos, a saber:

-

- 127-PPPGI-08 - *Políticas operativas específicas de seguridad y privacidad de la información*, ítem *Política de seguridad física y del entorno del centro de datos* (página 27). (Subrayado fuera de texto).

- Formato No. 127-FORGI-10 - *Control de acceso al centro de cómputo*. (Subrayado fuera de texto).

### 4.2.6 Objetivo de control A.9.4.5 (Control de acceso a códigos fuente de programas)

La OTIC almacena en repositorios GIT, alojados en la nube Azure, el código fuente de los aplicativos desarrollados, cuyo acceso está permitido únicamente a funcionarios y contratistas de dicha oficina, quienes están autorizados por el arquitecto de software o por el líder de desarrollo, mediante permisos de escritura o lectura. El control de acceso a la máquina virtual que alberga los repositorios GIT, está restringido únicamente al personal de infraestructura de TI. El acceso al código fuente de las aplicaciones sólo es posible desde la red local del DADEP o por medio de VPN, tal como se muestra en la imagen No. 8.

**Imagen No. 8. Acceso a repositorios GIT**

Fuente: OTIC

Se observaron quince (15) URL para las organizaciones GIT, entre ellas:

- CPM/MAP Sistema de Acciones Correctivas, Preventivas y de Mejora - http://integracion.dadep.gov.co/git/cpm

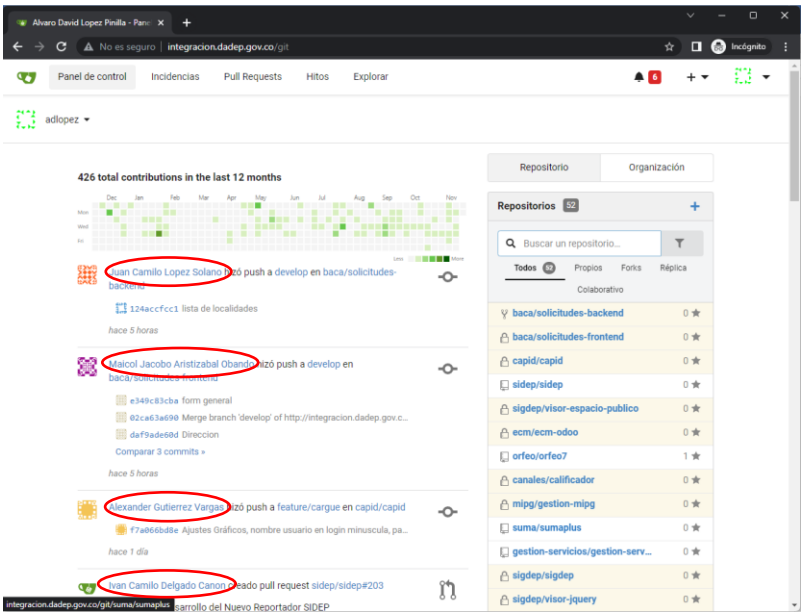
- Modelo Integrado de Planeación y Gestión - http://integracion.dadep.gov.co/git/mipg

- Sistema de Información de la Defensoría del Espacio Público - http://integracion.dadep.gov.co/git/sidep

- CPM/MAP Sistema de Acciones Correctivas, Preventivas y de Mejora - http://integracion.dadep.gov.co/git/cpm

Se evidenciaron los repositorios habilitados en la plataforma GIT para cuatro (4) ingenieros de la OTIC, como lo indica la imagen No. 9.

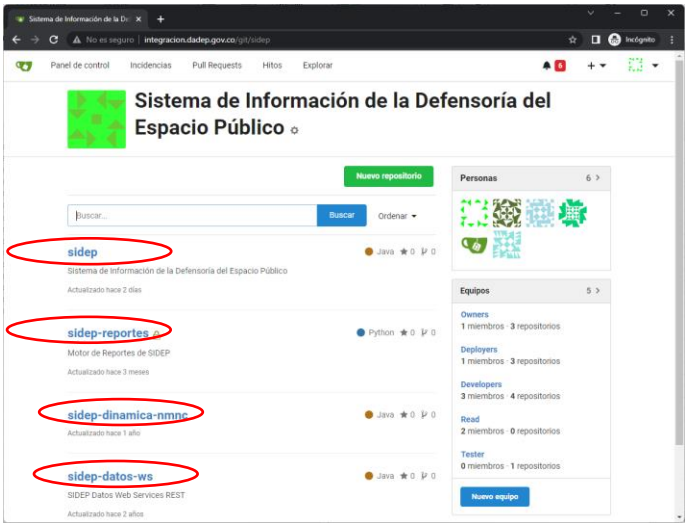
**Imagen No. 9. Repositorios habilitados para ingenieros OTIC**




Fuente: OTIC

Adicionalmente, cada organización GIT puede alojar varios repositorios de código fuente asociados, con diferentes permisos y roles de acceso, como lo indica la imagen No. 10.

**Imagen No. 10. Repositorios de código fuente**




Fuente: OTIC

### 4.2.7 Objetivo de control A.11.1.4 (Protección contra amenazas externas y ambientales)

Para la protección contra amenazas externas el sistema de seguridad perimetral está compuesto por:

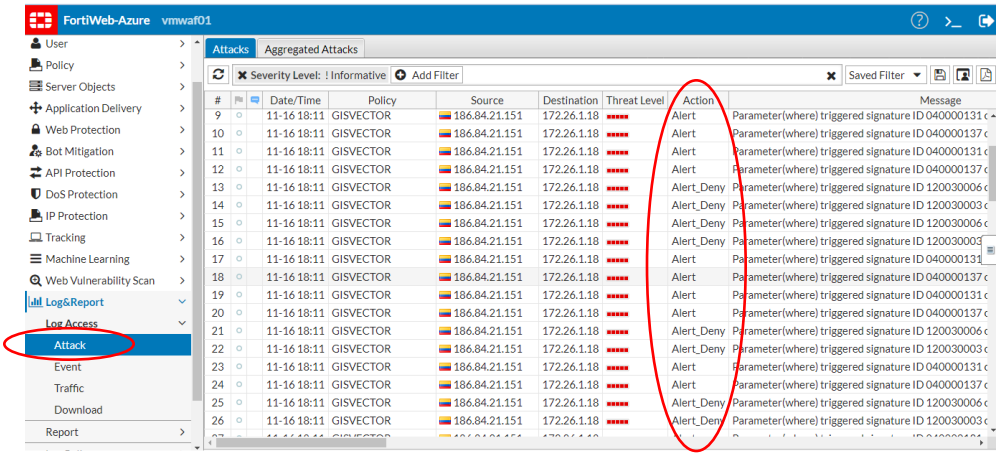
- Un (1) firewall para la nube de Oracle
- Un (1) firewall para la nube de Azure
- Dos (2) firewalls en HA on-premises, Ddos, Analyzer, Sandbox y firewall de aplicaciones web.

Para la red de datos se tienen tres (3) anillos de seguridad y uno de monitoreo a nivel de equipos de seguridad y de networking.

La mencionada infraestructura ha permitido consolidar un estado funcional y seguro de publicaciones web y monitoreo permanente a la red de datos, a través de los firewalls en HA y los equipos complementarios de la seguridad perimetral. Por lo anterior, la entidad ha protegido la publicación de los servicios web y los servicios internos, contra ataques de hackers como denegación de servicios, defacement, análisis de fuerza bruta, ataques dirigidos y de inyección de código, entre otros.

Se evidenció el monitoreo, control y bloqueo de ataques maliciosos, de acuerdo con las configuraciones de políticas de seguridad predefinidas en el firewall. La imagen No. 11 muestra en la columna *Action*, la alerta o denegación del acceso.

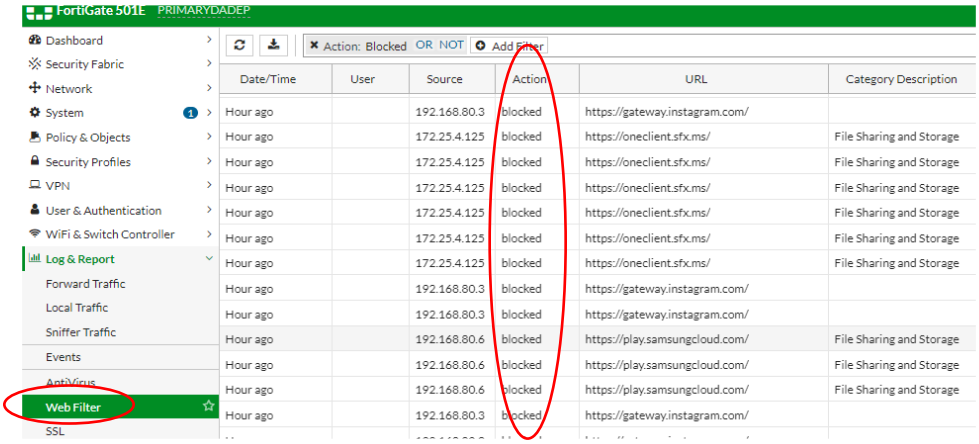
**Imagen No. 11. Control de ataques maliciosos**




Fuente: OTIC

La imagen No. 12 muestra los bloqueos que hace el firewall ante el intento de conexión a sitios inseguros.

**Imagen No. 12. Bloqueo de sitios inseguros**




| Date/Time | User | Source | Action | URL | Category Description |
|---|---|---|---|---|---|
| Hour ago | | 192.168.80.3 | blocked | https://gateway.instagram.com/ | |
| Hour ago | | 172.25.4.125 | blocked | https://oneclient.sfx.ms/ | File Sharing and Storage |
| Hour ago | | 172.25.4.125 | blocked | https://oneclient.sfx.ms/ | File Sharing and Storage |
| Hour ago | | 172.25.4.125 | blocked | https://oneclient.sfx.ms/ | File Sharing and Storage |
| Hour ago | | 172.25.4.125 | blocked | https://oneclient.sfx.ms/ | File Sharing and Storage |
| Hour ago | | 172.25.4.125 | blocked | https://oneclient.sfx.ms/ | File Sharing and Storage |
| Hour ago | | 172.25.4.125 | blocked | https://oneclient.sfx.ms/ | File Sharing and Storage |
| Hour ago | | 192.168.80.3 | blocked | https://gateway.instagram.com/ | |
| Hour ago | | 192.168.80.3 | blocked | https://gateway.instagram.com/ | |
| Hour ago | | 192.168.80.6 | blocked | https://play.samsungcloud.com/ | File Sharing and Storage |
| Hour ago | | 192.168.80.6 | blocked | https://play.samsungcloud.com/ | File Sharing and Storage |
| Hour ago | | 192.168.80.6 | blocked | https://play.samsungcloud.com/ | File Sharing and Storage |
| Hour ago | | 192.168.80.3 | blocked | https://gateway.instagram.com/ | |

Fuente: OTIC

La OTIC manifestó que durante lo corrido del año 2022 se presentaron tres (3) incidentes de amenazas de Phishing (engaño por suplantación de identidad) que fueron controlados oportunamente impidiendo la materialización del riesgo asociado.

Así las cosas, la infraestructura diseñada para la protección contra amenazas externas ha permitido estabilidad, seguridad y escalabilidad de los sistemas de información del DADEP.

En cuanto a la protección del Centro de Datos contra amenazas ambientales como incendios, la entidad cuenta con los siguientes elementos que contrarrestan posibles apariciones de humo o fuego:

- Un (1) sistema contraincendios compuesto por un panel de control de incendios con su fuente de poder.
- Una (1) estación manual de emergencia
- Un (1) botón de aborto de emergencia
- Dos (2) sensores detectores de humo
- Dos (2) boquillas para extinción con su respectiva tubería
- Un (1) cilindro con agente limpio
- Un panel de alarma con un módulo de luz estroboscópica acompañada de una sirena, ubicados en la puerta de ingreso del Centro de Datos.

Esta oficina no observó la existencia en el Centro de Cómputo de elementos o materiales como papel, cartón o plástico, que podrían facilitar la propagación de una eventual aparición de fuego.

### 4.2.8 Objetivo de control A.12.1.4 (Separación de los ambientes de desarrollo, pruebas y operación)

El software implementado por la entidad está debidamente organizado y separado en los ambientes de desarrollo, pruebas y producción (operación).

**Ambiente de desarrollo**

- Herramientas, IDEs y bases de datos para el desarrollo de código fuente, se instalan en el equipo de cómputo de cada desarrollador.
- Cargue continuo del código fuente generado al repositorio GIT de la entidad y de los scripts de bases de datos necesarios, por parte del desarrollador.
- Se evidenció la ubicación de la base de datos de desarrollo ORACLE para los aplicativos Sistema de Información de la Defensoría del Espacio Público (SIDEP) y Sistema Único para el Aprovechamiento del Espacio Público (SUMA+).

**Ambiente de pruebas**

- Servidores donde se instala el software desarrollado.
- Obtiene el código fuente desarrollado de los repositorios GIT de cada proyecto.
- Utiliza bases de datos centralizadas instaladas en otros servidores dentro de la red local.
- Funcionarios y contratistas acceden al nuevo software para realizar las pruebas técnicas y de aceptación.
- Los desarrolladores no tienen acceso a los despliegues del ambiente de pruebas.
- Se evidenciaron doce (12) ambientes de prueba de aplicaciones web, entre ellas: CAPID, ECM, Escuela del espacio público, ORFEO 7 pruebas, Portal inmobiliario, SIDEP pruebas y Sistema de plan anual de auditoría.

**Ambiente de producción**

- Servidores y componentes necesarios para la puesta en operación de una aplicación desarrollada y probada.
- Una vez aprobadas las pruebas técnicas y de aceptación de cada aplicación, son desplegadas en la nube de Azure.
- El despliegue incluye configuraciones de seguridad perimetral y publicación de certificados.
- Se evidenciaron veinte (20) ambientes de producción de aplicaciones o sistemas de información administrados por la OTIC, entre ellas: Portal web, Mesa de ayuda jurídica, Portal inmobiliario, SIDEP, ROYAL, Intranet y Control de horario.

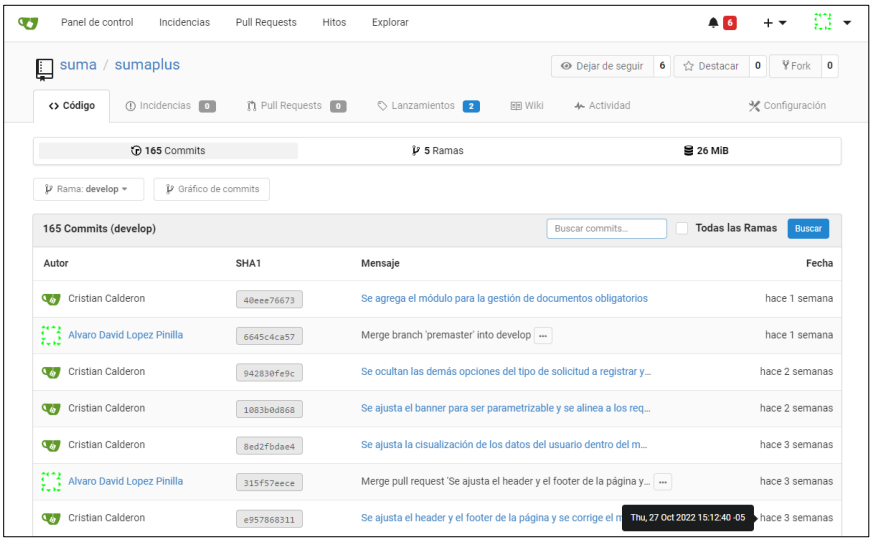
### 4.2.9 Objetivo de control A.14.2.2 (Procedimientos de control de cambios en sistemas)

El control de cambios utilizado en el desarrollo de software queda registrado en el repositorio GIT, donde se indica el nombre del desarrollador que hace el cambio y la fecha

respectiva del mismo. Adicionalmente, antes de colocar la aplicación en ambiente de producción se diligencia el formato de control de cambios No. 127-FORGI-20.

Para el aplicativo SUMA+ se evidenció un registro histórico de las modificaciones en el código fuente, donde se observan los nombres de los ingenieros desarrolladores que realizaron los cambios. Ver imagen No. 13.

**Imagen No. 13. Registro de modificaciones aplicativo SUMA+**




Fuente: OTIC

Adicionalmente, se evidenció el diligenciamiento del formato de control de cambios No. 127-FORGI-20 para el aplicativo SUMA+, que contiene, entre otra, la siguiente información:

- Ubicación del requerimiento
- Fecha de aprobación
- Descripción del cambio funcional
- Descripción del cambio técnico
- Impacto directo a otras aplicaciones
- Fecha de despliegue
- Resultado de las pruebas (Acta de aceptación de pruebas exitosas)

### 4.2.10 Objetivo de control A.16.1.6 (Aprendizaje obtenido de los incidentes de seguridad de la información)

La Oficina de Tecnologías de la Información y las Comunicaciones cuenta con una base de datos Excel que describe el nombre de la vulnerabilidad y la solución correspondiente, clasificadas según la criticidad: máxima, alta y media. Se evidenciaron 17 vulnerabilidades de criticidad máxima, 15 de alta y 9 de media.

Lo anterior, permite a la entidad reducir o evitar el impacto o la probabilidad de ocurrencia de incidentes futuros que afecten la seguridad de la información.

### 4.2.11 Consolidación objetivos de control

La tabla No. 2 consolida la aplicación de los controles según el Anexo A (Objetivos de control y Controles de referencia) de la Norma ISO/IEC 27001:2013.

**Tabla No. 2. Verificación de aplicación de los controles**

| Objetivos del control | Control | ¿Control aplicado? |
|---|---|---|
| **A.6.1.3** - Contacto con las autoridades | Se deben mantener contactos apropiados con las autoridades pertinentes. | Si |
| **A.6.2.1** - Política para dispositivos móviles | Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles. | Si (**pero debe fortalecerse**) |
| **A.6.2.2** - Teletrabajo | Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo. | Si |
| **A.8.3.1** - Gestión de medios removibles | Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización. | Si |
| **A.9.1.1** - Política de control de acceso | Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. | Si |
| **A.9.4.5** - Control de acceso a códigos fuente de programas | Se debe restringir el acceso a los códigos fuente de los programas. | Si |
| **A.11.1.4** - Protección contra amenazas externas y ambientales | Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. | Si |
| **A.12.1.4** - Separación de los ambientes de desarrollo, pruebas y operación | Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación. | Si |
| **A.14.2.2** - Procedimientos de control de cambios en sistemas | Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios. | Si |
| **A.16.1.6** - Aprendizaje obtenido de los incidentes de seguridad de la información | El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros. | Si |

Fuente: Anexo A, Norma ISO 27001:2013 – Elaboración OCI

## 5. CONCLUSIONES

De acuerdo con los resultados obtenidos durante el seguimiento, se concluye:

i. La Oficina de Tecnologías de la Información y Comunicaciones aplicó los controles de seguridad de la información que no permitieron la materialización de riesgos que afectaran la confidencialidad, integridad y disponibilidad de la información de la entidad, no obstante, se debe fortalecer el control de bloqueo de acceso a otros sitios como los juegos en línea.

ii. La no utilización de las herramientas de almacenamiento en la nube (OneDrive/SharePoint), ofrecidas por Microsoft 365, eventualmente puede ocasionar la pérdida de datos cuando técnicamente el disco duro sufre daños irreparables.

iii. Se identificaron documentos que hacen referencia distinta a los términos Centro de Datos y Centro de Cómputo, lo que podría llevar a una posible confusión en la conceptualización.

iv. La gestión de la seguridad de la información no está enfocada solamente a aspectos técnicos de la OTIC, su alcance cubre transversalmente todas las áreas, es decir, todo el personal de la entidad es responsable de su acatamiento y cumplimiento.

## 6. RECOMENDACIONES

De acuerdo con los resultados obtenidos durante el seguimiento, se recomienda:

i. Verificar permanentemente la aplicación de los controles de seguridad de la información para garantizar la continuidad de la operación de la entidad, fortaleciendo las medidas organizacionales que permitan prevenir violaciones de la seguridad.

ii. Revisar y fortalecer el control de acceso a otros sitios en Internet con el fin de evitar la eventual descarga de software malicioso.

iii. Socializar al interior de la entidad, con el apoyo de la Oficina Asesora de Comunicaciones, la utilización preventiva de las herramientas de almacenamiento en la nube adquiridas por la entidad, como OneDrive y/o SharePoint, con el fin de evitar la pérdida de datos.

iv. Homogeneizar en todos documentos relacionados con la utilización de los términos Centro de Datos y Centro de Cómputo, por aquella denominación que la OTIC considere la más apropiada técnicamente.

v. Actuar proactivamente y de manera oportuna ante eventuales incidentes de seguridad de la información que afecten la dinámica organizacional de la entidad.

**ALLAN MAURICE ALFISZ LÓPEZ**
Jefe Oficina de Control Interno

**JESÚS ALBEIRO RIZO GALLARDO**
Líder seguimiento

Copia: Diana Alejandra Rodríguez Cortés, Directora DADEP.
Syrus Asdrúbal Pacheco Vergel, Jefe OTIC.
Elaboró: Albeiro Rizo
Revisó y Aprobó: Allan Alfisz
Fecha: 29 de noviembre de 2022
Código: 130815